INTERNATIONAL DATA FLOWS: A *SCHREMS II* ASSESSMENT OF ELECTRONIC SURVEILLANCE LAWS IN AUSTRALIA

JOSHUA GACUTAN*

The Court of Justice of the European Union in Data Protection Commissioner v Facebook Ireland Ltd *acknowledged that European Union law on transfers of personal data from the European Economic Area to a third country is not deferential to that third country's national security powers. The ruling is of significant importance to Australia as it has no adequacy agreement with the European Union that would allow the free flow of personal data between their borders with limited data transfer safeguards. This article examines three case studies involving statutory powers that authorise Australian intelligence agencies to access and use non-citizens' personal data for national security purposes. This examination finds that the European Commission would likely consider these electronic surveillance laws to be barriers to an adequacy decision for Australia if an adequacy assessment is sought.*

CONTENTS

* BA LLB (Hons I) (Macq); Lawyer. I am grateful to Professor Douglas Guilfoyle and the anonymous reviewers for their helpful comments and feedback on earlier versions of this article. All views in this article are my own.

I Introduction

The Court of Justice of the European Union ('CJEU') has historically upheld a fundamental-rights-based approach to privacy and data protection.[1] As a result, the CJEU has applied European Union ('EU') privacy and data protection law to countries outside the EU, affirming the primacy of the rights of EU citizens over the interests of third countries and foreign companies.[2] Since 1995,

[1] See, eg, *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources* (Court of Justice of the European Union, C-293/12 and C-594/12, ECLI:EU:C:2014:238, 8 April 2014) [65]–[69] ('*Digital Rights Ireland*'); *Google Spain SL v Agencia Española de Protección de Datos* (Court of Justice of the European Union, C-131/12, ECLI:EU:C:2014:317, 13 May 2014) [96]–[99] ('*Google Spain*'); *Schrems v Data Protection Commissioner* (Court of Justice of the European Union, C-362/14, ECLI:EU:C:2015:650, 6 October 2015) [91]–[98] ('*Schrems I*'); *Data Protection Commissioner v Facebook Ireland Ltd* (Court of Justice of the European Union, C-311/18, ECLI:EU:C:2020:559, 16 July 2020) [168]–[199] ('*Schrems II*').

[2] See, eg, *Google Spain* (n 1). The CJEU applied the EU's *Data Protection Directive* to Google on specific grounds, in part because Google had an establishment in an EU member state: *Google Spain* (n 1) [49]. The CJEU found that what constitutes *processing* in the context of activities of a controller would include the activities of Google's subsidiary in Spain that sold advertising, even though the case was about Google Search which involved the collection and processing of data in the United States ('US'): at [50]–[57]. The CJEU's ruling confirmed a data subject's right to erasure (the so-called 'right to be forgotten'): at [100].

initially through the *Data Protection Directive* ('*DPD*'),[3] and, since 2018, the *General Data Protection Regulation* ('*GDPR*'),[4] one of the main mechanisms through which parties may transfer EU citizens' personal data to a country outside the European Economic Area ('EEA')[5] is when the European Commission ('EC')[6] certifies that the third country ensures 'an *adequate* level of protection'.[7] The effect of an adequacy decision is that personal data can flow from the EEA to the third country with limited data transfer safeguards.[8]

The influence of EU data protection law, especially the *GDPR*, on the domestic data privacy regimes of third countries has received significant attention in the literature.[9] A 2017 census of global data privacy laws conducted by Graham Greenleaf reported that 120 countries have enacted data privacy laws (in addition to 30 other countries that were considering draft legislation), with

[3] *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data* [1995] OJ L 281/31, art 25(1) ('*DPD*').

[4] *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)* [2016] OJ L 119/1, art 99 ('*GDPR*').

[5] The EEA 'was set up in 1994 to extend the EU's provisions on its internal market to the European Free Trade Area … countries', including Iceland, Liechtenstein, Norway and Switzerland: María Álvarez López and Ausra Rakstelyte, 'The European Economic Area (EEA), Switzerland and the North', *European Parliament* (Web Page, October 2021) <https://www.europarl.europa.eu/factsheets/en/sheet/169/the-european-economic-area-eea-switzerland-and-the-north>, archived at <https://perma.cc/DB3D-Z8M8>.

[6] The EC 'has the power to determine, on the basis of article 45 of [the *GDPR*] whether a country outside the EU offers an adequate level of data protection': 'Adequacy Decisions: How the EU Determines if a Non-EU Country Has an Adequate Level of Data Protection', *European Commission* (Web Page) <https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en>, archived at <https://perma.cc/FSX8-A4TW>. The adoption of an adequacy decision involves: (1) a proposal from the EC; (2) an opinion of the European Data Protection Board; (3) an approval from representatives of EU countries; and (4) the adoption of the decision by the EC.

[7] *GDPR* (n 4) art 45(1) (emphasis added).

[8] Ibid art 46(1).

[9] See, eg, Anu Bradford, 'The Brussels Effect' (2012) 107(1) *Northwestern University Law Review* 1; Paul M Schwartz, 'Global Data Privacy: The EU Way' (2019) 94(4) *New York University Law Review* 771; Graham Greenleaf, '"European" Data Privacy Standards Implemented in Laws Outside Europe' [2018] *University of New South Wales Law Research Series* 2:1–4, 1 ('European Data Privacy Standards'); Graham Greenleaf, '"GDPR Creep" for Australian Businesses but Gap in Law Widens' [2018] *University of New South Wales Law Research Series* 54:1–4, 1; Michael L Rustad and Thomas H Koenig, 'Towards a Global Data Privacy Standard' (2019) 71(2) *Florida Law Review* 365.

many of the laws bearing similarities with EU data protection law.[10] Even if third countries are not expressly legislating EU-style data privacy laws, EU regulatory law scholar, Anu Bradford, hypothesises that global regulatory convergence towards the *GDPR*'s standards is taking place due to a 'de facto *Brussels Effect*'.[11] Bradford explains that '[w]hile the EU regulates only its internal market, multinational corporations often have an incentive to standardize their production globally and adhere to a single rule'.[12] It follows that multinational companies adapt their processes to comply with the *GDPR*'s higher standards, and are then incentivised to lobby their respective governments to adopt the *GDPR*'s standards to level the playing field against their domestic competitors.[13]

The *GDPR*'s influence on the privacy reform discourse in Australia is clear.[14] In the Australian Competition and Consumer Commission's ('ACCC's') final report for the Digital Platforms Inquiry, the ACCC recommended major reforms to Australia's federal information privacy law — the *Privacy Act 1988* (Cth) ('*Privacy Act*').[15] A number of these reforms are influenced by the *GDPR*'s standards and received immediate support from the federal government and inclusion in the Attorney-General's Department's ('AGD's') broader review of the *Privacy Act*.[16] In line with the ACCC's proposed reforms, and as evidence

[10] See Graham Greenleaf, 'Global Data Privacy Laws 2017: 120 National Data Privacy Laws, Including Indonesia and Turkey' [2017] *University of New South Wales Law Research Series* 45:1–8, 1, 3–4. See also Graham Greenleaf, 'The Influence of European Data Privacy Standards outside Europe: Implications for Globalization of Convention 108' (2012) 2(2) *International Data Privacy Law* 68, 72–7. Greenleaf states that 'something reasonably described as "European standard" data privacy laws are becoming the norm in most parts of the world with data privacy laws': at 77.

[11] Bradford (n 9) 6 (emphasis added). Cf Schwartz (n 9). Paul Schwartz argues that, instead of Bradford's Brussels Effect hypothesis, there is a 'varied range of nation-state, transnational, and corporate behavior that has helped spread EU data protection throughout the world': at 773.

[12] Bradford (n 9) 6.

[13] Ibid.

[14] See Greenleaf, 'European Data Privacy Standards' (n 9) 3–4.

[15] Australian Competition and Consumer Commission, *Digital Platforms Inquiry* (Final Report, June 2019) 34–5.

[16] The final report stated that

> the ACCC does not propose wholesale adoption of the *GDPR* in this Report, but rather particular recommendations to address key findings of the Inquiry (some of which reflect key features and principles of the *GDPR*, for example recommendation 16(c)).

Ibid 439. The recommendations which are influenced by the *GDPR* (n 4) are as follows: recommendation 16(a), '[u]pdate the definition of "personal information" in the *Privacy Act* to clarify that it captures technical data such as IP addresses, device identifiers, location data,

of the Brussels Effect hypothesis, submissions by businesses and industry groups to the AGD's review of the *Privacy Act* support the enactment of those *GDPR*-style provisions proposed by the ACCC in order to strengthen Australia's adequacy prospects.[17] Several submissions[18] also justify the removal of the small business and employee records exemptions in the *Privacy Act* because the Article 29 Data Protection Working Party, the EU's former data protection advisory body, considered those exemptions to be likely barriers to an adequacy decision for Australia in 2001.[19]

and any other online identifiers that may be used [to] identify an individual': *Digital Platforms Inquiry* (n 15) 34; recommendation 16(c), at 35:

> Strengthen consent requirements and pro-consumer defaults … Valid consent should require a clear affirmative act that is freely given, specific, unambiguous and informed (including about the consequences of providing or withholding consent).

Recommendation 16(d) is to, '[e]nable the erasure of personal information' to

> [require] APP entities to erase the personal information of a consumer without undue delay on receiving a request for erasure from the consumer, unless the retention of information is necessary for the performance of a contract to which the consumer is a party, is required under law, or is otherwise necessary for an overriding public interest reason.

Ibid 35. Recommendation 16(e) is to '[g]ive individuals a direct right to bring actions and class actions against APP entities in court to seek compensation for an interference with their privacy under the *Privacy Act*'. See also Australian Government, *Regulating in the Digital Age: Government Response and Implementation Roadmap for the Digital Platforms Inquiry* (Report, 12 December 2019) 11–13.

[17] See, eg, Interactive Games & Entertainment Association, Submission to Attorney-General's Department, *Review of the Privacy Act 1988 (Cth)* (November 2020) 18–20. The Interactive Games & Entertainment Association, which represents the interests of Australian and New Zealand video game companies, stated in its submission, at 19, that

> the best approach for achieving free, open and safe cross-border information flows is to ensure that any necessary and appropriate changes to Australian privacy laws are as consistent as possible [with] those of larger markets, such as the EU.

[18] See, eg, ibid 10; KPMG Australia, Submission to the Attorney-General's Department, *Review of the Privacy Act 1988 (Cth)* (December 2020) 6; Deakin University and Centre for Cyber Security Research and Innovation, Submission to Attorney-General's Department, *Review of the Privacy Act 1988 (Cth)* (November 2020) [7], [14], [52].

[19] European Commission Article 29 Data Protection Working Party, *Opinion 3/2001 on the Level of Protection of the Australian Privacy Amendment (Private Sector) Act 2000*, 5095/00/EN WP40 (26 January 2001) 3–4, 6. For a discussion of the Article 29 Data Protection Working Party's opinion of the *Privacy Amendment (Private Sector) Act 2000* (Cth), see Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice* (Report No 108, May 2008) vol 2, 1068–9 [31.21] (citations omitted) ('*For Your Information*'):

> One of the main drivers behind the *Privacy Amendment (Private Sector) Act 2000* (Cth) was to facilitate trade with European countries by having the *Privacy Act* deemed adequate for the purposes of the EU Directive. In March 2001, however, the Working Party released an opinion expressing concern that some sectors and activities are excluded from the protection of the *Privacy Act*, including small businesses and employee records. The Working

Even if these recommendations raise the *Privacy Act* closer to the *GDPR*'s standards, any reforms proposed as part of moving towards adequacy under the *GDPR* must consider the position of Australia's National Intelligence Community ('NIC') agencies and the breadth of their statutory powers as judged in light of the CJEU's ruling in *Data Protection Commissioner v Facebook Ireland Ltd* ('*Schrems II*').[20] The CJEU in *Schrems II* invalidated the EC's adequacy decision — *Commission Decision 2016/1250*[21] — which approved the EU–US Privacy Shield, a mechanism on which thousands of United States ('US') and EU companies based their personal data transfers.[22] The CJEU's fundamental rationale for invalidating the EU–US Privacy Shield involved concerns that US surveillance programs authorised under § 702 of the *Foreign Intelligence*

Party found that, without further safeguards, the Australian standards could not be deemed equivalent to the EU Directive.

[20] *Schrems II* (n 1). The NIC includes the Office of National Intelligence, the Australian Signals Directorate, the Australian Geospatial-Intelligence Organisation, the Australian Secret Intelligence Service, the Australian Security Intelligence Organisation, the Defence Intelligence Organisation, the Australian Criminal Intelligence Commission, as well as the intelligence functions of the Australian Federal Police, Australian Transaction Reports and Analysis Centre, and the Department of Home Affairs: 'The National Intelligence Community', *Office of National Intelligence* (Web Page) <https://www.oni.gov.au/national-intelligence-community>.

[21] *Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the EU–US Privacy Shield* [2016] OJ L 207/1, recital 13 ('*EU–US Privacy Shield Adequacy Decision*').

[22] *Schrems II* (n 1) [201]. The CJEU's invalidation of the *EU–US Privacy Shield Adequacy Decision* (n 21) caused a major rift to the $7.1 trillion transatlantic economic relationship: Wilbur Ross, 'US Secretary of Commerce Wilbur Ross Statement on Schrems II Ruling and the Importance of EU–US Data Flows' (Press Release, US Department of Commerce, 16 July 2020) <https://2017-2021.commerce.gov/index.php/news/press-releases/2020/07/us-secretary-commerce-wilbur-ross-statement-schrems-ii-ruling-and.html>, archived at <https://perma.cc/8N65-GDWE>. Many of Silicon Valley's largest data-driven companies such as Google, Meta and YouTube depend on access to, and use of, EU citizens' personal data to provide their services in the EU and therefore, by extension, depend on the EU–US Privacy Shield: see 'Privacy Shield List', *Privacy Shield Framework* (Web Page) <https://www.privacyshield.gov/list>, archived at <https://perma.cc/6QJL-45VN>. There have been efforts to revamp the EU–US Privacy Shield to ensure compliance with *Schrems II* (n 1). On 25 March 2021, the EU Commissioner for Justice, Didier Reynders, and the US Secretary of Commerce, Gina Raimondo, announced that the EU and US had decided to 'intensify negotiations on an enhanced EU–US Privacy Shield framework' that would be compliant with *Schrems II* (n 1): Didier Reynders and Gina Raimondo, 'Intensifying Negotiations on Transatlantic Data Privacy Flows: A Joint Press Statement by European Commissioner for Justice Didier Reynders and US Secretary of Commerce Gina Raimondo' (Press Release STATEMENT/21/1443, European Commission, 25 March 2021). The joint statement also pointed out the EU and US's 'shared commitment to privacy, data protection and the rule of law and [their] mutual recognition of the importance of transatlantic data flows to [their] respective citizens, economies, and societies'.

Surveillance Act of 1978 ('*FISA*')[23] and *Exec Order No 12333* ('*EO-12333*')[24] did not provide 'essentially equivalent' protections for EU citizens to those guaranteed under EU law.[25] The CJEU reasoned that § 702 of the *FISA* and *EO-12333*, taken together, did not provide for: (i) a proportionality assessment sufficient to ensure collection and use of EU citizens' personal data by US intelligence agencies is limited to what is strictly necessary;[26] and (ii) effective legal remedies for EU citizens if their personal data is misused in the course of US surveillance programs.[27] As a consequence of the CJEU's ruling, third countries seeking an adequacy decision must demonstrate limitations and safeguards that are 'essentially equivalent' to those guaranteed under EU law.[28] These limitations and safeguards must be available in circumstances where EU citizens' personal data is accessed and used by public authorities for national security and law enforcement purposes.[29]

Against this backdrop, this article argues that certain electronic surveillance laws in Australia would likely be considered barriers to an adequacy decision in light of the *Schrems II* ruling. This article begins, in Part II, by situating EU privacy and data protection law within the normative context of the EU's governance philosophy. It then outlines the *GDPR*'s international data transfer provisions, and proceeds to identify the CJEU's key criticisms of US surveillance activities in *Schrems II*. Having set the background, the main analysis in this article is undertaken in the remaining two parts. Part III examines three case studies where the Australian Signals Directorate ('ASD') and the Australian Security Intelligence Organisation ('ASIO') have statutory powers to collect non-citizens' personal data offshore, intercept personal data over telecommunications systems onshore, and access metadata retained by telecommunications providers. Each case study is assessed against two threshold questions used by the CJEU to assess the compatibility of electronic surveillance laws with EU law. Those threshold questions are: (i) whether the relevant statutory power

[23] 50 USC § 1881a (2018).

[24] *Exec Order No 12333*, 3 CFR 212 (1982) ('*EO-12333*').

[25] *Schrems II* (n 1) [180]–[185], [201].

[26] Ibid [184].

[27] Ibid [191]–[193], [195]–[197].

[28] Ibid [203].

[29] See, eg, *Commission Implementing Regulation (EU) 2021/1772 of 28 June 2021 Pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the Adequate Protection of Personal Data by the United Kingdom* [2021] OJ L 360/1, recitals 3, 112 ('*UK Adequacy Decision*'); *Commission Implementing Decision (EU) 2021/1773 of 28 June 2021 Pursuant to Directive (EU) 2016/680 of the European Parliament and of the Council on the Adequate Protection of Personal Data by the United Kingdom* [2021] OJ L 360/69, recital 159 ('*UK Law Enforcement Directive Adequacy Decision*').

employs proportionality considerations to ensure access and use of non-citizens' personal data is limited to what is strictly necessary; and (ii) whether non-citizens are afforded effective legal remedies against misuse of their personal data in the third country. Part IV concludes that the case studies cast doubt on Australia's adequacy decision prospects under the *GDPR*, because each regime falls considerably short of providing 'essentially equivalent' protections to those guaranteed under EU law. Finally, this article posits that the case studies highlight not only a wider 'adequacy' gap overlooked by the present *Privacy Act* reform discourse, as well as the consequentialist treatment of privacy protection in Australia.

II The CJEU's Ruling in *Schrems II*

In order to consider Australia's adequacy prospects in light of the CJEU's ruling in *Schrems II*, it is necessary to briefly describe the EU's governance philosophy and situate EU privacy and data protection law within this normative context. Framing the EU's approach to privacy and data protection around deontological ethics assists in understanding the standard of privacy and data protection that third countries must guarantee to ensure 'an *adequate* level of protection' under the *GDPR*.[30] Part II, therefore, will outline the deontological commitments in EU privacy and data protection law. It will then describe *GDPR* provisions regarding international data transfers, then proceed to identify the CJEU's key criticisms of US surveillance activities in *Schrems II*.

A *Deontological Commitments in EU Privacy and Data Protection Law*

Historically, there have been two accounts that have applied to determine the extent and shape of privacy protection — namely, deontological and consequentialist approaches.[31] Although no legal and political system is an absolute embodiment of one single account, the EU's approach to privacy and data protection can be understood as grounded in deontological ethics.[32] For deontologists, the value of privacy protection is determined by the extent to which the protection engenders basic moral rights and duties such as individual

[30] *GDPR* (n 4) art 45(1) (emphasis added).

[31] See David Lindsay, 'An Exploration of the Conceptual Basis of Privacy and the Implications for the Future of Australian Privacy Law' (2005) 29(1) *Melbourne University Law Review* 131, 134–5 ('Conceptual Basis of Privacy').

[32] Ibid 146, 169.

autonomy, control and dignity.[33] By comparison, consequentialist bases are variable, such that the extent of protecting privacy interests hinges on what is considered desirable for society in the circumstances.[34] Consequentialist approaches are achieved by determining what is 'good' and then defining 'the right' that will promote 'the good'.[35] If 'the good', for example, is to ensure collective security, then a consequentialist account would only justify ensuring individual privacy interests to the extent that it aligns with the overarching goal of collective security.

Deontological accounts may be grounded in Kantian ethics, which assert that at the core of dignity is the idea that each individual should be treated as an end in themselves, and never simply as a means to furthering another person's or society's ends.[36] For instance, one basis on which deontologists may object to privacy laws with consequentialist aims of maximising efficiency in data processing is out of concern for the potential for such 'data processing to undermine the respect [of] individuals as self-determining, autonomous moral agents'.[37] It follows that deontological accounts often confer a higher standard of privacy protection than consequentialist accounts, because an invasion of privacy is 'generally impermissible', even if it would produce desirable net outcomes for society.[38]

A number of scholars have argued that Europe's distinct cultural trajectory and history have led to the deontological values of individual autonomy, control and dignity being ascribed the highest normative value.[39] One driving force, in the context of privacy and data protection rights, arises from Europe's memory of the Nazi Holocaust, the Stasi, and political repression in Warsaw Pact

[33] Ibid 144, 146; Neil MacCormick, *Legal Right and Social Democracy: Essays in Legal and Political Philosophy* (Oxford University Press, 1982) 144.

[34] Lindsay, 'Conceptual Basis of Privacy' (n 31) 149.

[35] Ibid 144.

[36] See, eg, ibid 146; Stanley I Benn, 'Privacy, Freedom, and Respect for Persons' in J Roland Pennock and John W Chapman (eds), *Privacy* (Atherton Press, 1971) 1, 16–26; Julie E Cohen, 'What Privacy Is for' (2013) 126(7) *Harvard Law Review* 1904, 1906–7.

[37] Lindsay, 'Conceptual Basis of Privacy' (n 31) 161.

[38] Ibid 148.

[39] Several scholars have interrogated the roots of the EU's rights-focused discourse. For example, James Whitman traced the emergence of privacy rights from continental, political and cultural developments of the idea that honour, personal reputation and dignity are central to human flourishing: James Q Whitman, 'The Two Western Cultures of Privacy: Dignity versus Liberty' (2004) 113(6) *Yale Law Journal* 1151, 1164–89. Whitman argues that the European culture of dignity is the result of a centuries-long revolt against the aristocratic and monarchical styles of status privilege stemming from the 17th and 18th centuries, and he claims that '[o]ver time, it has come to seem unacceptable that only certain persons should enjoy legal protections for their "dignity"': at 1166.

countries, and 20th-century totalitarian regimes, which seized troves of state-held personal data to facilitate atrocities, mass oppression and surveillance.[40] Against this background, for example, the Constitutional Court in Germany in the seminal 1983 population census decision held that data protection rights flow from the individual's right to 'informational self-determination' which is itself based on the rights to human dignity and free development of personality in the German Basic Law.[41] The idea of informational self-determination 'serves to promote [an] individual's right to personality (whether through freedom from unauthorized surveillance or by facilitating individual self-presentation)'.[42]

Privacy law scholar Joel Reidenberg explains that the EU's rights-based conception of privacy and data protection as fundamental rights derives from the EU's governance philosophy which is anchored in social and citizen protection.[43] Under this governance philosophy, Reidenberg explains that the state becomes

> the necessary player to frame the social community in which individuals develop, and information practices must serve individual identity. Citizen autonomy, in this view, effectively depends on a backdrop of legal rights.[44]

The EU's governance philosophy does not merely constrain a government's own processing but requires positive government action to empower individuals' self-serving informational practices and identities.[45] EU citizens, therefore, become the ultimate bearer of privacy and data protection rights.[46] Therefore,

[40] Rustad and Koenig (n 9) 372–3.

[41] Orla Lynskey, 'Deconstructing Data Protection: The "Added-Value" of a Right to Data Protection in the EU Legal Order' (2014) 63(3) *International and Comparative Law Quarterly* 569, 592; Bundesverfassungsgericht [German Constitutional Court], 1 BvR 209/83, 15 December 1983 reported in (1983) 65 BVerfGE 1 [tr 'Judgment of 15 December 1983: 1 BvR 209/83', *Bundesverfassungsgericht* (Web Page, 2021) <https://www.bundesverfassungsgericht.de/EN/Homepage/home_node.html>, archived at <https://perma.cc/57PT-LJG5>].

[42] Lynskey (n 41) 591. See also Stefano Rodotà, 'Data Protection as a Fundamental Right' in Serge Gutwirth et al (eds), *Reinventing Data Protection?* (Springer, 2009) 77, 78–80.

[43] Joel R Reidenberg, 'Resolving Conflicting International Data Privacy Rules in Cyberspace' (2000) 52(5) *Stanford Law Review* 1315, 1347.

[44] Ibid (citations omitted).

[45] Ibid; Paul M Schwartz and Karl-Nikolaus Peifer, 'Transatlantic Data Privacy Law' (2017) 106(1) *Georgetown Law Journal* 115, 126.

[46] Schwartz and Peifer (n 45) 126. See, eg, Věra Jourová, 'How Does the Data Protection Reform Strengthen Citizens' Rights?', *Publications Office of the European Union* (Factsheet, 10 January 2016) <https://op.europa.eu/s/vSFN>, archived at <https://perma.cc/U4VP-DEXM>. Věra

various EU constitutional documents and treaties establish privacy and data protection as fundamental rights.[47] The *European Convention on Human Rights* ('*ECHR*') firmly enshrined privacy as a fundamental human right in post-war Europe.[48] Article 8 of the *ECHR* grants the individual a 'right to respect for … private and family life'[49] and aims to ensure protection from interference from public authorities of an individual's private life, including their home and correspondence.[50] The EU's key constitutional document — the *Charter of Fundamental Rights of the European Union* ('*EU Charter*')[51] — contains a privacy right in similar terms to the *ECHR* and establishes a separate right to data protection which sits alongside, and in addition to, the right to privacy in the *EU Charter*.[52] Article 8(1) of the *EU Charter* provides '[e]veryone has the right to the protection of personal data'.[53] Finally, the *Treaty on the Functioning of the European Union*, which entered into force in 2009,[54] reiterated the centrality of data

Jourová, the former EU Commissioner for Justice, Consumers and Gender Equality, emphasised that the commencement of the *GDPR* (n 4) in 2016 would 'strengthen citizens' rights': Jourová (n 46). The European Parliament also presented the *GDPR* (n 4) as 'put[ting] the citizen back in the driving seat': European Parliament, 'New EU Rules on Data Protection Put the Citizen Back in the Driving Seat' (Press Release, 17 December 2015) 1.

47 See, eg, *Charter of Fundamental Rights of the European Union* [2016] OJ C 202/393, arts 7–8 ('*EU Charter*'); *Convention for the Protection of Human Rights and Fundamental Freedoms*, opened for signature 4 November 1950, 213 UNTS 221 (entered into force 3 September 1953) art 8 ('*ECHR*').

48 *ECHR* (n 47) art 8.

49 Ibid art 8(1).

50 The European Court of Human Rights, which supervises the enforcement of the *ECHR* (n 47), has over time expanded the scope of art 8 to include specific rights regarding data protection: Lee A Bygrave, 'Data Protection Pursuant to the Right to Privacy in Human Rights Treaties' (1998) 6(3) *International Journal of Law and Information Technology* 247, 255–6.

51 *EU Charter* (n 47).

52 Ibid arts 7–8. Article 7 recognises general privacy protection for individuals by granting all Europeans 'the right to respect for his or her private and family life, home and communications'.

53 Article 8 of the *EU Charter* (n 47) not only distinguishes data protection from privacy, but also lays down some specific guarantees in [2]–[3] — namely, that personal data 'must be processed fairly for specified purposes and on the basis of the consent of the person concerned or [on] some other legitimate basis laid down by law'; that '[e]veryone has the right of access to data which has been collected concerning him or her, and the right to have it rectified'; and that '[c]ompliance with these rules shall be subject to control by an independent authority'.

54 *Treaty on European Union*, opened for signature 7 February 1992, [1992] OJ C 191/1 (entered into force 1 November 1993), as amended by *Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Community*, opened for signature 13 December 2007, [2007] OJ C 306/1 (entered into force 1 December 2009) ('*Treaty of Lisbon*'). The *Treaty of Lisbon* (n 54) amendment resulted in the *Treaty on the Functioning of the European Union*, opened for signature 7 February 1992, [2016] OJ C 202/1 (entered into force 1 November 1993) art 16 ('*FEU*').

protection in EU law.[55] Article 16 states that '[e]veryone has the right to the protection of personal data concerning them'.[56] That right complements the right to data protection in art 8 of the *EU Charter* and guarantees the competence of the EU to regulate data protection for the EU, including member states.[57]

It is contended below that the CJEU's rulings in *Schrems v Data Protection Commissioner* ('*Schrems I*')[58] and *Schrems II* reflect deontological commitments in affirming the primacy of EU citizens' privacy and data protection rights. While there are other more nuanced justifications for EU privacy and data protection law,[59] introducing the core deontological and consequentialist accounts of privacy is appropriate for the purpose of relating the findings of the case studies in Part III to a broader discussion around the weaknesses of the consequentialist treatment of privacy protection in Australia in Part IV.

B GDPR*: International Personal Data Transfers from the EEA to Third Countries*

The EU's *GDPR* regulates the collection and use of personal data and provides data subjects a range of data rights over their personal data.[60] Articles 44–5 of the *GDPR* provide that EU citizens' personal data may only be transferred from the EEA to third countries if specific conditions are met.[61] The rationale for these conditions is to prevent EU citizens from losing the protections afforded

[55] *FEU* (n 54).

[56] Ibid art 16(1). See also art 1(2) of the *GDPR* (n 4), which establishes that all 'natural persons' have a fundamental 'right to the protection of personal data'. Article 4(1) of the *GDPR* (n 4) defines 'personal data' as 'any information relating to an identified or identifiable natural person', which is defined broadly as

> one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person …

[57] *FEU* (n 54) art 16(2).

[58] *Schrems I* (n 1).

[59] For a comprehensive overview of the different approaches to the conceptualisation of privacy and data protection, see Megan Richardson, *Advanced Introduction to Privacy Law* (Edward Elgar, 2020).

[60] *GDPR* (n 4) arts 15–20. Key data subject rights include a right to information on the personal data being held by a controller, including how it is stored, the right to rectification and a right to the erasure of personal data (the so-called 'right to be forgotten'): at arts 15–17. Regarding the so-called 'right to explanaton' in the *GDPR* (n 4), see Joshua Gacutan and Niloufer Selvadurai, 'A Statutory Right to Explanation for Decisions Generated Using Artificial Intelligence' (2020) 28(3) *International Journal of Law and Information Technology* 193, 193–216.

[61] *GDPR* (n 4) arts 44–50 are also applicable to international organisations.

to them if their data is transferred to a third country that provides a lower level of protection.[62]

1 *Adequacy Findings*

Article 45 provides the core 'adequacy' principle by establishing that any transfer of personal data to a third country shall only take place if the EC has issued a decision certifying that the third country ensures 'an adequate level of protection'.[63] The standard against which 'an adequate level of protection' is measured is that set by EU law, notably the *GDPR*, as well as the CJEU's case law.[64] The CJEU in *Schrems I* held that 'an adequate level of protection' does not necessarily mean an identical level of protection to the one guaranteed by EU law, but a 'level of protection of fundamental rights and freedoms that is *essentially equivalent*' to that guaranteed within the EU.[65] This means that the mechanisms in which third countries provide 'recourse for protecting personal data may differ from … ones employed in the European Union, as long as they prove, in practice, effective for ensuring an adequate level of protection'.[66]

Article 45(2) provides an extensive — though non-exhaustive — list of factors to be considered by the EC in its adequacy assessment of the level of protection provided by a third country, including:

[62] *Schrems II* (n 1) [92]–[93]. See also Christopher Kuner, *Transborder Data Flows and Data Privacy Law* (Oxford University Press, 2013) 103–4; Julian Wagner, 'The Transfer of Personal Data to Third Countries under the GDPR: When Does a Recipient Country Provide an Adequate Level of Protection?' (2018) 8(4) *International Data Privacy Law* 318, 318–20.

[63] *GDPR* (n 4) art 45(1). The EC has only recognised a limited number of countries as providing adequate protection. National adequacy decisions include Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea, Switzerland, the United Kingdom and Uruguay: 'Adequacy Decisions: How the EU Determines if a Non-EU Country Has an Adequate Level of Data Protection', *European Commission* (Web Page) <https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en>, archived at <https://perma.cc/F94A-2XD9>. EC adequacy decisions may also apply to particular categories, including sectors within a third country that have agreed to particular data protection standards. For example, the *EU–US Privacy Shield Adequacy Decision* (n 21) was not a finding of national adequacy but a finding that the Privacy Shield itself provided adequate protection for personal data transferred to self-certified US organisations: at recital 13.

[64] *UK Adequacy Decision* (n 29) recitals 2–4. The EC also states that '[t]he European Data Protection Board's … adequacy referential is also of significance in this regard': at recital 3.

[65] *Schrems I* (n 1) [73] (emphasis added).

[66] *UK Adequacy Decision* (n 29) recital 4. The EC explained that

> the [adequacy standard] lies in whether, through the substance of data protection rights and their effective implementation, supervision and enforcement, the foreign system as a whole delivers the required level of protection.

1 The rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data is being transferred;[67]

2 The existence and effective functioning of one or more independent supervisory authorities in the third country;[68] and

3 The international commitments the third country has entered into.[69]

In addition to art 45(2), recital 104 provides that the EC in its assessment of 'the third country, or of a territory or [a] specified sector within a third country', should,

> [in] line with the fundamental values on which the Union is founded, in particular the protection of human rights … take into account how a particular third country respects the rule of law, access to justice as well as international human rights norms and standards and its general and sectoral law, *including legislation concerning public security, defence and national security* as well as public order and criminal law.[70]

In sum, an adequacy decision is

> based on a comprehensive analysis of the third country's legal order, covering both the rules applicable to … data importers and the limitations and safeguards as regards access to personal data by public authorities.[71]

On the whole, an adequacy decision signals that the third country to which it applies provides an 'essentially equivalent' level of protection to an EU member state, resulting in the free flow of personal data from the EEA to the third country without the need for one of the data transfer safeguards or permissible derogations described below.

2 *Additional Data Transfer Safeguards and Derogations*

In the absence of an adequacy decision, transfers of personal data to a third country are permitted under art 46 if additional safeguards are provided.[72] The main safeguards are binding corporate rules, standard contractual clauses

[67] *GDPR* (n 4) art 45(2)(a).

[68] Ibid art 45(2)(b).

[69] Ibid art 45(2)(c).

[70] Ibid recital 104 (emphasis added).

[71] *UK Adequacy Decision* (n 29) recital 3.

[72] *GDPR* (n 4) art 46(1).

('SCCs'), an approved code of conduct, or an approved certification mechanism.[73] When no adequacy decision or appropriate safeguards are in place, the remaining mechanism is through so-called derogations from the *GDPR*.[74] Under EU law, however, derogations from general rules are interpreted narrowly and therefore can only be relied on exceptionally.[75]

C Schrems II: *Invalidation of the EU–US Privacy Shield Adequacy Decision*

It is necessary to briefly discuss the CJEU's 2015 ruling in *Schrems I* as background as *Schrems II* is a continuation of those proceedings.

1 *Background*

In 2013, Edward Snowden, a former National Security Agency ('NSA') contractor, leaked a cache of documents allegedly describing the surveillance programs of the NSA, specifically PRISM and UPSTREAM,[76] to journalists from *The*

[73] Ibid arts 46(2)(b)–(f).

[74] Ibid art 49. These permissible situations include the transfer of personal data with the explicit consent of the data subject, transfers necessary for the performance of a contract between the data subject and the controller, and transfers necessary for the public interest purposes: at arts 49(1)(a)–(b), (d).

[75] The wording of *GDPR* (n 4) art 49 and the guidelines of the European Data Protection Board ('EDPB') make clear that these derogations are to be strictly interpreted: European Data Protection Board, *Guidelines 2/2018 on Derogations of Article 49 under Regulation 2016/679* (Guidelines, 25 May 2018) 4. In *Schrems I* (n 1) [92], the Court stated that 'derogations and limitations in relation to the protection of personal data [are] to apply only in so far as is strictly necessary'. See also *Dashiqiao Sanqiang Refractory Materials Co Ltd v Council of the European Union* (Court of Justice of the European Union, C-15/12 P, ECLI:EU:C:2013:572, 19 September 2013) [17]; *European Commission v Ireland* (Court of Justice of the European Union, C-82/10, ECLI:EU:C:2011:621, 29 September 2011) [44].

[76] 'PRISM' is a code name for a program under which the NSA collects the content of electronic communications, including phone calls and emails, where the persons are 'reasonably believed' to be non-US citizens located outside the US: Sergei Boeke and Quirine AM Eijkman, 'State Surveillance in Cyberspace: A New Perspective on Digital Data Practices by Intelligence and Security Services' in Lee Jarvis, Stuart Macdonald and Thomas M Chen (eds), *Terrorism Online: Politics, Law and Technology* (Routledge, 2015) 125, 129. 'UPSTREAM collection' is a term used by the NSA for collecting internet communications 'while Internet traffic is in transit from one unspecified location to another': Edward C Liu, Andrew Nolan and Richard M Thompson II, *Overview of Constitutional Challenges to NSA Collection Activities* (CRS Report No R43459, 21 May 2015) 10. The communications were collected from 'fibre-optic cables and other infrastructure carrying Internet traffic': Royal United Services Institute for Defence and Security Studies, *A Democratic Licence to Operate: Report of the Independent Surveillance Review* (Report No 2-15, July 2015) 48 ('*RUSI Report*').

Guardian, *The Washington Post* and other publications.[77] The NSA conducted these surveillance programs by either collecting data directly from undersea telecommunications cables and servers that carry them or by compelling telecommunications providers and private companies to supply the data.[78] Following Snowden's disclosure, privacy activist Maximilian Schrems complained to the Data Protection Commissioner in Ireland ('DPC') that Facebook Ireland was transferring EU personal data to Facebook Inc's US servers in breach of the EU's *DPD*, which prohibited transfers to a third country that did not ensure an 'adequate level of protection'.[79] Specifically, Schrems challenged the EC's adequacy decision — *Commission Decision 2000/520* (the so-called '*EU–US Safe Harbour Decision*').[80] After the Irish DPC refused to investigate Schrems's

[77] See Edward Snowden, *Permanent Record* (Metropolitan Books, 2019) 250–1; Rebecca Sanders, *Plausible Legality: Legal Culture and Political Imperative in the Global War on Terror* (Oxford University Press, 2018) 143.

[78] See generally Ian Brown et al, 'Toward Multilateral Standards for Foreign Surveillance Reform' in Russell A Miller (ed), *Privacy and Power: A Transatlantic Dialogue in the Shadow of the NSA-Affair* (Cambridge University Press, 2017) 461, 461–2; *RUSI Report* (n 76) 2 [0.7]; TC Sottek and Janus Kopfstein, 'Everything You Need to Know about PRISM', *The Verge* (Web Page, 17 July 2013) <https://www.theverge.com/2013/7/17/4517480/nsa-spying-prism-surveillance-cheat-sheet>, archived at <https://perma.cc/8KJN-BFJV>.

[79] *DPD* (n 3) art 25(1). In a press release, the CJEU stated that Schrems's complaint took the view that

> in the light of the revelations made in 2013 by Edward Snowden concerning the activities of the United States intelligence services (in particular the National Security Agency ('the NSA')), the law and practice of the United States do not offer sufficient protection against surveillance by the public authorities …

Court of Justice of the European Union, 'The Court of Justice Declares that the Commission's US Safe Harbour Decision Is Invalid' (Press Release No 117/15, 6 October 2015) <https://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf>, archived at <https://perma.cc/8KHN-H4BV>.

[80] *Commission Decision of 26 July 2000 Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the Safe Harbour Privacy Principles and Related Frequently Asked Questions Issued by the US Department of Commerce* [2000] OJ L 215/7 ('*EU–US Safe Harbour Decision*'); *Schrems I* (n 1) [1]. The *EU–US Safe Harbour Decision* (n 80) arose out of a document developed by the US Department of Commerce and the EU Commission containing the Safe Harbour Privacy Principles and a list of frequently asked questions for US companies. This mechanism allowed US companies to 'self-certify' their compliance with the Safe Harbour Privacy Principles to the US Department of Commerce and, in effect, their guarantee of providing an 'adequate level of protection' under the *DPD* (n 3) (now *GDPR* (n 4)): Lindsay, 'Conceptual Basis of Privacy' (n 31) 175; *Schrems I* (n 1) [82].

complaint, Schrems took his complaint to the High Court of Ireland, which subsequently referred questions to the CJEU for a preliminary ruling.[81]

In *Schrems I*, the CJEU invalidated the *EU–US Safe Harbour Decision* because it did not afford 'essentially equivalent' protection for personal data to that guaranteed under EU law, in violation of arts 7 and 8 of the *EU Charter*.[82] Significantly, the CJEU referred to the inadequate concessions and findings of the EC about the adequate protection of personal data in the *EU–US Safe Harbour Decision*, rather than establishing any deficits in US surveillance law itself.[83] The CJEU also pointed to the primacy of US law in the *EU–US Safe Harbour Decision*, which carried a provision that 'national security, public interest, or law enforcement requirements' have precedence over the Safe Harbour Privacy Principles.[84]

Following *Schrems I*, Facebook Ireland explained that most of its personal data transfers to US servers were based on SCCs under *Commission Decision 2010/87*.[85] Schrems then reformulated his complaint to the Irish DPC and argued that Facebook Ireland's reliance on SCCs were not valid due to US law compelling telecommunications providers and private companies to provide access to EU citizens' personal data to US intelligence agencies.[86] However, after

[81] *Schrems I* (n 1) [28]–[36]. A reference for a preliminary ruling allows the courts and tribunals of the EU member states, in disputes which have been brought before them, to refer questions to the CJEU about the interpretation of EU law or the validity of an EU act: *Recommendations to National Courts and Tribunals, in Relation to the Initiation of Preliminary Ruling Proceedings* [2016] OJ C 439/1, 1 [1]. Although the CJEU does not decide the dispute itself, a preliminary ruling is binding on all EU courts: 'Preliminary Ruling Proceedings: Recommendations to National Courts', *EUR-Lex: Access to European Union Law* (Web Page, 31 October 2017) <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=legissum:l14552>, archived at <https://perma.cc/PKW3-ZJER>. The CJEU's preliminary ruling also dealt with the question of the scope of powers of the national data protection authorities: *Schrems I* (n 1) [40]–[66]. However, for present purposes this article will focus on the invalidation of the *EU–US Safe Harbour Decision* (n 80).

[82] *Schrems I* (n 1) [91], [96]–[98], [104]–[106].

[83] Ibid [83].

[84] Ibid [84], quoting *EU–US Safe Harbour Decision* (n 80) annex I. See also *Schrems I* (n 1) [85]–[89].

[85] *Schrems II* (n 1) [74].

[86] Ibid [55]. Based on Schrems's revised complaint, the Irish DPC raised several questions before the High Court of Ireland, which then referred 11 questions to the CJEU for a preliminary ruling: at [68]. For present purposes, this article will focus on the CJEU's ruling in respect of the EU–US Privacy Shield.

Schrems lodged his complaint, the EC adopted *Commission Decision 2016/1250*, which approved the EU–US Privacy Shield.[87]

2 *Decision*

In *Schrems II*, the CJEU declared the EU–US Privacy Shield invalid on the basis that the access and use of EU citizens' personal data by US intelligence agencies under US surveillance programs permitted under § 702 of the *FISA* and *EO-12333* were not restricted in a way that met protections which were 'essentially equivalent' to those provided for in the EU.[88] The CJEU's finding may be summarised into two primary grounds.

First, the CJEU found the limitations and safeguards on the powers of US intelligence agencies under US surveillance law failed to respect the principle of proportionality under art 52(1) of the *EU Charter*.[89] The CJEU, in particular, observed that US surveillance programs authorised under § 702 of the *FISA* and *EO-12333* did not ensure that data collection and use by US intelligence agencies were limited to what is strictly necessary under EU law, therefore interfering with the rights to privacy and data protection under arts 7 and 8 of the *EU Charter*.[90] In this regard, the CJEU observed that under § 702 of the *FISA*, the Foreign Intelligence Surveillance Court is limited to 'verify[ing] whether those surveillance programmes [targeting non-US persons] relate to the objective of acquiring foreign intelligence information' and 'does not cover the issue of whether "individuals are properly targeted to acquire foreign intelligence information"'.[91] Accordingly, the CJEU held that § 702 of the *FISA* could not ensure a level of protection essentially equivalent to that guaranteed by the principle of proportionality in art 52(1) of the *EU Charter*, because the provision does not indicate any limitations on the power it confers to implement surveillance programs or the existence of guarantees for non-US persons

[87] *EU–US Privacy Shield Adequacy Decision* (n 21) recital 13. The EU–US Privacy Shield was essentially a 'self-certification' regime whereby EU and EEA companies were able to legally transfer personal data to US-based companies that were listed in the EU–US Privacy Shield: at recitals 14–16.

[88] *Schrems II* (n 1) [184]–[185], [201]–[202].

[89] Ibid [168]–[185]. Article 52(1) of the *EU Charter* (n 47), entitled 'Scope and interpretation of rights and principles', states:

> Any limitation on the exercise of the rights and freedoms recognised by this *Charter* must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.

[90] *Schrems II* (n 1) [169], [174], [184].

[91] Ibid [179], quoting *EU–US Privacy Shield Adequacy Decision* (n 21) recital 109.

subject to those programs.[92] In a similar manner, the CJEU dismissed *EO-12333*, which authorised access to data in transit to the US, because it did not 'delimit in a sufficiently clear and precise manner the scope of such bulk collection of personal data'.[93]

Secondly, the CJEU found that, contrary to what is required under art 47 of the *EU Charter*, EU citizens lack legal recourse in the US when their personal data is misused by US intelligence agencies.[94] The CJEU stated that the surveillance programs permitted under § 702 of the *FISA* and *EO-12333* do not grant 'data subjects rights actionable in the courts against the US authorities, from which it follows that data subjects have no right to an effective remedy'.[95] In this respect, the CJEU commented that 'the very existence of effective judicial review designed to ensure compliance with provisions of EU law is inherent in the existence of the rule of law'.[96] The CJEU then continued to identify deficiencies in the US Privacy Ombudsperson mechanism introduced by the EU–US Privacy Shield.[97] The CJEU emphasised that data subjects must have the

> possibility of bringing legal action before an independent and impartial court in order to have access to their personal data, or to obtain the rectification or erasure of such data.[98]

The CJEU, however, found that the US Privacy Ombudsperson mechanism lacked substantive guarantees of the Ombudsperson's independence from the executive and any power to adopt decisions binding on intelligence services.[99] Consequently, the CJEU observed that EU citizens are left with no possibility

92 *Schrems II* (n 1) [180], [185].

93 Ibid [183].

94 Ibid [190]–[197]. Article 47 of the *EU Charter* (n 47), entitled 'Right to an effective remedy and to a fair trial', states:

> Everyone whose rights and freedoms guaranteed by the law of the Union are violated has the right to an effective remedy before a tribunal in compliance with the conditions laid down in this Article. Everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal previously established by law. Everyone shall have the possibility of being advised, defended and represented. Legal aid shall be made available to those who lack sufficient resources in so far as such aid is necessary to ensure effective access to justice.

95 *Schrems II* (n 1) [192].

96 Ibid [187]. The CJEU further noted that 'legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him or her [fails to] respect the essence of the fundamental right to effective judicial protection'.

97 Ibid [193]–[197].

98 Ibid [194].

99 Ibid [195]–[196].

of legal recourse before an oversight body that can provide essentially equivalent remedies to those required by art 47 of the *EU Charter*.[100]

D *Conclusion*

The CJEU in *Schrems I* and *Schrems II* consistently referred to the fundamental rights enshrined in the *EU Charter* to define the appropriate contours of access by public authorities of third countries to EU personal data under the *GDPR*. So, any interference with arts 7 and 8 of the *EU Charter* must be provided for by law and limited to what is strictly necessary under art 52(1) of the *EU Charter*, and ensure effective judicial protection for EU citizens under art 47 of the *EU Charter*.[101] In essence, the CJEU affirmed the rights of EU citizens over the national security interests of the US, thereby reflecting the deontological commitments in respect of privacy and data protection as fundamental rights.

The CJEU's ruling in *Schrems II* has evoked a number of criticisms. One criticism is that the ruling entails considerable hypocrisy because EU intelligence agencies directly benefit from information sharing with US intelligence agencies.[102] Another criticism is that the ruling imposes double standards and, in some instances, a higher standard for third countries.[103] That argument is based on the view that very few EU member states provide protections for non-citizens subject to their national security surveillance practices equivalent to those under EU law.[104] Notwithstanding the merits of these arguments, the fact remains that, however erroneous or fallible its reasoning, the *Schrems II* ruling is *final*. Consequently, third countries seeking an adequacy decision must demonstrate limitations and safeguards that are 'essentially equivalent' to those

[100] Ibid [197].

[101] Ibid [174], [178], [186].

[102] Adam Klein, 'Statement by Chairman Adam Klein on the Terrorist Finance Tracking Program' (Media Release, Privacy and Civil Liberties Oversight Board, 19 November 2020) 1, 4:

> Many of those programs produce significant benefits for European allies, in addition to unilateral benefits for the United States. For example, US agencies frequently share valuable intelligence produced under Section 702 of the *Foreign Intelligence Surveillance Act* with their European counterparts … Transatlantic discussions about surveillance and privacy could be improved by greater candor about what each side is doing, and why. Ultimately, Americans and Europeans face the same challenge: protecting our societies in a manner consistent with fundamental values and the rule of law.

[103] Zuzanna Gulczyńska, 'A Certain Standard of Protection for International Transfers of Personal Data under the GDPR' (2021) 11(4) *International Data Privacy Law* 360, 366, 372.

[104] Ibid 371–2. In the context of the CJEU's ruling in *Schrems I* (n 1), see also Paul Roth, '"Adequate Level of Data Protection" in Third Countries Post-*Schrems* and under the *General Data Protection Regulation*' (2017) 25(1) *Journal of Law, Information and Science* 49, 63–4.

guaranteed under EU law with regard to access and use of EU citizens' personal data by public authorities.[105]

III Assessment of Electronic Surveillance Law Case Studies

Australia has a complex legislative framework that governs when and how NIC agencies can access and use personal data to carry out their functions.[106] Part III will examine three case studies where the ASD and ASIO have statutory powers authorising the access and use of non-citizens' personal data against the CJEU's ruling in *Schrems II*. It will first provide a brief overview and justification for selecting the case studies, before proceeding to an assessment against the threshold questions that arose in *Schrems II*. Those threshold questions are: (i) whether the relevant statutory power employs proportionality considerations to ensure access and use of non-citizens' personal data is limited to what is strictly necessary under art 52(1) of the *EU Charter*; and (ii) whether non-citizens are provided effective legal remedies against the misuse of their personal data in the third country under art 47 of the *EU Charter*.

Parts III and IV draw on Dennis Richardson's *Comprehensive Review of the Legal Framework of the National Intelligence Community* ('*Richardson Review*').[107] The *Richardson Review* is significant as it is the first comprehensive inquiry into the NIC since the Hope Royal Commissions of 1974 and 1983.[108] The *Richardson Review* is also extensive due to the advent of electronic surveillance, growth of NIC agencies since the Hope Royal Commissions, and the sheer number of national security laws that have been enacted following 11 September 2001.[109] Accordingly, this article refers to the findings of the *Richardson Review* where relevant when examining each case study.

[105] *UK Adequacy Decision* (n 29) recitals 2–3.

[106] Dennis Richardson, *Comprehensive Review of the Legal Framework of the National Intelligence Community* (Report, December 2019) vol 1, 33 [3.7] ('*Richardson Review*').

[107] Ibid.

[108] Ibid vol 1, 32 [3.1]. The Royal Commission on Intelligence and Security ('First Hope Royal Commission') of 1974 examined the ASIO's functions, structure, and treatment of human sources: 'The Hope Royal Commissions', *Australian Security Intelligence Organisation* (Web Page, 2021) <https://www.asio.gov.au/about/history/hope-royal-commissions.html>, archived at <https://perma.cc/SFT9-2KS5>. The Royal Commission on Australia's Security and Intelligence Agencies ('Second Hope Royal Commission') of 1983 examined the operations, conduct, performance, control and accountability of Australia's intelligence agencies.

[109] *Richardson Review* (n 106) vol 1, 33 [3.9], 43–4 [3.62], 87 [5.4]. The *Richardson Review* (n 106) notes that '[b]etween [11 September 2001] and 1 August 2019, the Parliament passed more than 124 Acts amending the legislative framework for the NIC, making more than 14,500

A *Justification and Overview of Case Studies*

The case studies are selected because *Schrems II* was a concerted attack on § 702 of the *FISA* and *EO-12333*.[110] As discussed in Part II, the CJEU accepted that the provisions effectively permitted the NSA (which is ordinarily authorised to collect signals intelligence and data)[111] to undertake *bulk* collection and processing of personal data overseas, including non-US citizens' personal data in transit to the US. To that end, the case studies involve similar circumstances where the ASD and ASIO has statutory powers to access non-citizens' personal data offshore, intercept personal data over telecommunications systems onshore and access metadata retained by telecommunications providers.

The first case study concerns the ASD's collection of signals intelligence outside Australia under the *Intelligence Services Act 2001* (Cth) ('*Intelligence Services Act*'). The *Intelligence Services Act* provides the ASD with intelligence gathering powers to carry out its functions, including to obtain intelligence about the capabilities, intentions and activities of people or organisations outside of Australia.[112] The ASD was established in 2018 as an 'independent statutory agency within the Defence portfolio reporting directly to the Minister for Defence'.[113] The primary function of the ASD is to provide foreign signals intelligence to the Australian Defence Force and the Australian Government to support military and strategic decision-making.[114] The ASD also advises federal and state government agencies on information and cyber security risks, as well

individual amendments … inclusive of the minor and technical': at vol 1, 33 [3.9]. See also Kent Roach, *The 9/11 Effect: Comparative Counter-Terrorism* (Cambridge University Press, 2011) 310; George Williams, 'A Decade of Australian Anti-Terror Laws' (2011) 35(3) *Melbourne University Law Review* 1136, 1144–6.

110 *Schrems II* (n 1) [178]–[185], [191]–[192].

111 *EO-12333* (n 24) § 1.7(c)(1), as inserted by *Exec Order No 13470*, 3 Fed Reg 45325, 45326 (2008).

112 *Intelligence Services Act 2001* (Cth) s 11(1) ('*Intelligence Services Act*'). The Act limits ASD intelligence collection to the 'capabilities, intentions or activities of people or organisations outside Australia'.

113 Explanatory Memorandum, Intelligence Service Amendment (Establishment of the Australian Signals Directorate) Bill 2018 (Cth) [1].

114 'About ASD', *Australian Signals Directorate* (Web Page) <asd.gov.au/about>, archived at <https://perma.cc/N5L8-JZL6>; *Intelligence Services Act* (n 112) s 7(1). The documents leaked by Edward Snowden reportedly revealed that the ASD and NSA 'conducted a surveillance operation on Indonesia during the United Nations climate change conference in Bali in 2007', and that 'Australian diplomatic facilities throughout the Asia-Pacific region were involved in an NSA-led covert signals intelligence program': Dan Jerker B Svantesson and Rebecca Azzopardi, 'Systematic Government Access to Private-Sector Data in Australia' in Fred H Cate and James X Dempsey (eds), *Bulk Collection: Systematic Government Access to Private-Sector Data* (Oxford University Press, 2017) 221, 239–40.

as coordinating responses to cyber attacks and providing code-breaking and encryption assistance to government agencies.[115]

The second case study concerns the ASIO's collection of foreign intelligence about non-citizens in Australia under the *Australian Security Intelligence Organisation Act 1979* (Cth) ('*ASIO Act*').[116] The ASIO was established in 1949 as Australia's domestic counter-intelligence and security service.[117] Although the ASIO's collection of foreign intelligence onshore is not its core focus, such collection complements the functions of the ASD, which is limited to obtaining foreign intelligence offshore.[118] The *ASIO Act* and *Telecommunications (Interception and Access) Act 1979* (Cth) ('*Telecommunications Interception Act*') provide a framework where an authorised ASIO officer can obtain a telecommunications service warrant, named-person warrant and a foreign communications warrant[119] from the Attorney-General to intercept live communications passing over a telecommunications system to collect foreign intelligence on non-citizens in Australia.[120] Foreign intelligence collection warrants allow the ASIO to collect emails, telephone calls and SMS messages that pass across or are stored on telecommunications networks.[121] These warrants cannot be issued to collect information concerning an Australian citizen or permanent resident.[122]

The third case study concerns Australia's mandatory data retention regime ('MDRR'), which commenced in 2015 under the *Telecommunications*

115 'About ASD' (n 114); *Intelligence Services Act* (n 112) ss 7(1)(ca), (e), (2)(a)–(b).

116 *Australian Security Intelligence Organisation Act 1979* (Cth) ss 17(1)(e), 27A ('*ASIO Act*').

117 'The Establishment of ASIO', *Australian Security Intelligence Organisation* (Web Page) <https://www.asio.gov.au/about/history/establishment-asio.html>, archived at <https://perma.cc/YR98-MPWN>.

118 *ASIO Act* (n 116) s 17.

119 Notably, a foreign communications warrant is distinct from the other two warrants in that it authorises an ASIO officer to conduct interception in Australia that is directed at collecting communications to or from people who are located outside Australia: *Telecommunications (Interception and Access) Act 1979* (Cth) ss 5 (definition of 'foreign communication'), 11C(1), 12 ('*Telecommunications Interception Act*').

120 Ibid ss 11A–11C. Section 27A of the *ASIO Act* (n 116) also authorises the ASIO to exercise its other warrant powers, such as its search, computer access, surveillance device, interception and inspection of postal and delivery service articles warrant powers to collect foreign intelligence. Section 4 of the *ASIO Act* (n 116) (definition of 'foreign intelligence') provides that foreign intelligence includes '[i]ntelligence about the capabilities, intentions and activities of people or organisations outside Australia' (such as foreign governments).

121 *Telecommunications Interception Act* (n 119) ss 11A–11C, 109.

122 Ibid s 11D(5); *ASIO Act* (n 116) s 27A(9).

Interception Act.[123] Unlike the statutory powers of the ASD and ASIO described above, the MDRR does not discriminate between the personal data of Australians and non-citizens.[124] The MDRR requires carriers, carriage service providers and internet service providers (together, 'telecommunications providers') to retain telecommunications data for at least two years and provide access to that data for certain NIC agencies, including the ASIO.[125] The retained data (so-called 'metadata') includes subscriber account details (including devices) and the source, destination, date, time, duration, location and type of communication.[126] When metadata is combined with other types of data held by NIC agencies, such as social media interactions, vehicle tolls, video surveillance and electronic transactions, NIC agencies can create a comprehensive digital profile of individuals, tracking their associations with others, their movements and activities at practically any given time.[127]

B *Proportionality under art 52(1) of the* EU Charter

The first threshold question concerns whether each statutory power employs proportionality considerations to ensure data collection and use are limited to what is strictly necessary under art 52(1) of the *EU Charter*. In order to meet this threshold, the CJEU prescribed that the legislation in question

> must lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards, so that the persons whose data has been transferred have sufficient guarantees to protect effectively

[123] The MDRR came into effect in 2015 with the enactment of the *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015* (Cth) ('*Telecommunications Interception Amendment Act*'): Law Council of Australia, Submission to Parliamentary Joint Committee on Intelligence and Security, *Review of the Mandatory Data Retention Regime* (18 July 2019) 5 [2]. Prior to the regime's commencement, the Parliamentary Joint Committee on Intelligence and Security ('PJCIS') warned that the regime

> raises fundamental privacy issues, and is arguably a significant extension of the power of the state over the citizen. No such regime should be enacted unless those privacy … concerns are sufficiently addressed.

Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, *Inquiry into Potential Reforms of Australia's National Security Legislation* (Report, May 2013) 7 [1.35], 190 [5.208].

[124] *Telecommunications Interception Act* (n 119) ss 187A–187AA.

[125] Ibid pt 5-1A div 1, as inserted by *Telecommunications Interception Amendment Act* (n 123) sch 1 pt 1; Commonwealth, *Parliamentary Debates*, House of Representatives, 30 October 2014, 12560–3 (Malcolm Turnbull, Minister for Communications).

[126] *Telecommunications Interception Act* (n 119) s 187AA(1).

[127] Peter Leonard, 'Mandatory Internet Data Retention in Australia: Looking the Horse in the Mouth after It Has Bolted' (2015) 101 (June) *Intellectual Property Forum* 43, 47.

> their personal data against the risk of abuse. It must, in particular, indicate in what circumstances and under which conditions a measure providing for the processing of such data may be adopted, thereby ensuring that the interference is limited to what is strictly necessary.[128]

Thus, the following assessment will examine whether the statutory powers set out any objective criteria and circumstances that effectively limit the ASD's and ASIO's access and use of non-citizens' personal data to what is strictly necessary to carry out their functions.

1 *Australian Signals Directorate*

The Australian Parliament has omitted any concept of proportionality in relation to the ASD's collection of signals intelligence on non-citizens under the *Intelligence Services Act*. The absence of proportionality considerations is a deliberate policy choice and is not an accident.[129] In s 14 of the *Intelligence Services Act*, for example, Parliament has expressly legislated on the basis that it can immunise officers of intelligence agencies, including the ASD, from consequences of intelligence activities undertaken overseas that are unlawful under the laws of another country. This provision ensures the ASD's operational effectiveness because it would unduly constrain the ASD's ability to carry out its functions if officers were required to comply with the privacy and data protection laws of countries subject to their operations. Accordingly, the ASD's intelligence gathering powers are broad in scope and can, in a practical sense, enable the bulk collection of non-citizens' personal data.

The practical manifestation of Parliament's omission of proportionality considerations for non-citizens is evidenced in the clear distinction between Australians and non-citizens in the *Intelligence Services Act*. This bifurcation has the effect of prescribing at least two procedural protections for Australians that are subject to the ASD's intelligence activities overseas. The first protection is in the form of consideration and authorisation by the Minister for Defence before the ASD can undertake activities for the specific purpose of producing intelligence on an Australian person, or for activities that will have a direct effect on an Australian person.[130] To make this authorisation, the Minister must be

128 *Schrems II* (n 1) [176].

129 *Richardson Review* (n 106) vol 1, 231 [10.33]–[10.34].

130 *Intelligence Services Act* (n 112) ss 8–9. Section 8(1)(a)(i) requires the responsible Minister to issue a written direction requiring the agency to obtain an authorisation under s 9 before 'undertaking an activity … for the specific purpose, or for purposes which include the specific purpose, of producing intelligence on an Australian person'. The Minister for Defence is the Minister responsible for the ASD: 'Leadership', *Australian Signals Directorate* (Web Page) <https://www.asd.gov.au/about/leadership>, archived at <https://perma.cc/9MJ5-AQYF>.

satisfied that the ASD's activities will be necessary and reasonable.[131] In addition, the Minister must be satisfied that the Australian person or persons targeted by the activities are likely to be involved in one of a range of serious activities — for example, activities that pose a significant risk to a person's safety, are likely to be a threat to security, or are related to the proliferation of weapons of mass destruction.[132] The second protection is in the form of the Minister's 'written privacy rules on how ASD is to protect the privacy of *Australians*'[133] so as to preserve their privacy as far as is consistent with the proper performance of the ASD's functions.[134] There is no equivalent legislative requirement for the Minister to make privacy rules for non-citizens. However, even if the Minister were to amend the ASD's privacy rules to include similar guidelines for non-citizens, the privacy rules are not legislative instruments and can be amended without any Parliamentary oversight, including in relation to the protections they offer Australians.[135]

2 *Australian Security Intelligence Organisation*

The *ASIO Act* provides two forms of limitations for the ASIO's collection of foreign intelligence on non-citizens in Australia. The first limitation is foreign intelligence collection warrants.[136] Before the Attorney-General can issue these warrants,[137] he or she must be satisfied on the basis of advice from the Minister for Defence or Minister for Foreign Affairs that the collection of the foreign intelligence 'is in the interests of Australia's national security, Australia's foreign relations or Australia's national economic well-being'.[138] These expressions, however, do not, in the words of the CJEU in *Schrems II*, appropriately 'indicate … in what circumstances and under which conditions' the ASIO's warranted powers may be used to target non-citizens.[139] For example, the term 'Australia's

131 *Intelligence Services Act* (n 112) ss 9(1)(a)–(c). Section 9 sets out the preconditions for giving authorisation, including the requirement in s 9(1)(a) that the Minister must be satisfied that 'any activities which may be done in reliance on the authorisation will be necessary for the proper performance of a function of the agency concerned'.

132 Ibid ss 9(1A)(a)(i), (iii)–(iv).

133 'Accountability', *Australian Signals Directorate* (Web Page) <https://www.asd.gov.au/accountability>, archived at <https://perma.cc/S2D8-HB2L> (emphasis added).

134 *Intelligence Services Act* (n 112) ss 15(1)–(2).

135 Ibid s 15(7).

136 *ASIO Act* (n 116) s 27A.

137 Minister for Home Affairs, *Minister's Guidelines in Relation to the Performance by the Australian Security Intelligence Organisation of Its Functions and the Exercise of Its Powers* (Guidelines, August 2020) 8 [2.8] ('*Minister's Guidelines*').

138 *ASIO Act* (n 116) s 27A(1)(b).

139 *Schrems II* (n 1) [176].

national economic well-being' is not defined in the *Intelligence Services Act*. The term is not expanded on or meaningfully referred to in the Explanatory Memorandum to the Intelligence Services Bill 2001 (Cth) or the Minister's second reading speech.[140] In other legislation where the term is referred to, such as the *National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018* (Cth), the term captures a wide range of conduct beyond the provision's plain meaning to encompass direct threats to the Australian economy that have national security implications.[141] The low threshold required for the Attorney-General's issuance of foreign intelligence collection warrants underscores the view that the government's obligation to protect the privacy of Australians does not extend to non-citizens, especially in the context of foreign surveillance activities.[142] Indeed, the *Richardson Review* found that, because foreign intelligence collection warrants do not target Australians, 'the need for a threshold that reflects the particular intrusiveness of each individual activity is less pronounced'.[143] Consequently, this limitation does not set out objective criteria by which to constrain the ASIO's foreign collection on non-citizens in Australia to what is strictly necessary for the ASIO to carry out its functions.

The second limitation is in the form of the Minister for Home Affairs' guidelines to the Director-General of Security.[144] The Minister's guidelines provide limitations on the ASIO's collection of intelligence, including personal data.[145] Under the Minister's guidelines, '[i]nformation is to be [obtained] by [the] ASIO in a lawful, timely and efficient way', and in accordance with a number of

[140] Commonwealth, *Parliamentary Debates*, House of Representatives, 27 June 2001, 28635–9 (Alexander Downer, Minister for Foreign Affairs).

[141] National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017 (Cth) cl 82.7(d)(ii). See Explanatory Memorandum, National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017 (Cth) 64 [350]:

> Subparagraph 82.7(d)(ii) refers to harm or prejudice to Australia's economic interests. The term 'prejudice' is intended to capture a broad range of intended conduct, including an intention to harm or injure Australia's economic interests or to cause disadvantage to Australia. The term is also intended to cover impairment or loss to Australia's economic interests. The prejudice to Australia's economic interests is not required to be serious or substantial but is intended to be more than a minor or trivial prejudice that has no long-lasting effect on Australia's overall economy.

[142] *Richardson Review* (n 106) vol 1, 231–2 [10.35]–[10.38].

[143] Ibid vol 2, 95 [19.85]. See also at vol 1, 232 [10.38]:

> [The] collection and use of intelligence should not unduly or disproportionately interfere with human rights, especially those of Australians. … [T]he privacy of Australians [ranks] highly in the protection to be accorded to human rights.

[144] *ASIO Act* (n 116) ss 8A(1)–(2); 'Minister's Guidelines', *Australian Security Intelligence Organisation* (Web Page) <https://www.asio.gov.au/ministers-guidelines.html>, archived at <https://perma.cc/Q94E-44WE>.

[145] *Minister's Guidelines* (n 137) 11–16 [3.1]–[4.15].

proportionality criteria.[146] The guidelines provide that the 'intrusiveness of techniques or methods for collecting information are to be considered in determining approval levels for their use', such that the more intrusive the investigative technique, the higher the level of officer that should be required to approve its use.[147] Further, the guidelines state that the Director-General of Security 'will take all reasonable steps to ensure that the ASIO's collection, retention, use, handling, and disclosure of personal information is limited to what is reasonably necessary to perform its functions'.[148] Like the ASD's privacy rules, however, the guidelines are not legislative instruments.[149] There is also no obligation for the Minister to provide the guidelines to the Director-General of Security.[150] Taken together, the threshold required to be met for the issuance of foreign intelligence collection warrants and the Minister's guidelines as practical *guidance*, are insufficient under art 52(1) of the *EU Charter*.

3 *Mandatory Data Retention Regime*

The MDRR arguably exceeds art 52(1) of the *EU Charter* on at least three grounds, such that the interferences to individual privacy are not proportionate to the regime's legitimate aim of protecting Australia from the most serious crime and terrorism.[151]

First, when an authorised officer of an enforcement agency seeks access to metadata from a telecommunications provider, the general rule is that they must be satisfied on reasonable grounds that any interference with the privacy of any individual or individuals that may result from the disclosure or use of the metadata is justifiable and proportionate, having regard to a specific set of proportionality criteria under the *Telecommunications Interception Act*.[152] While the proportionality criteria are comparable to those in the *EU Charter*, the ease of access to metadata for a broad range of law enforcement agencies, without any third-party oversight body vetting the disclosures of metadata,

[146] Ibid 11 [3.4]. These proportionality criteria include, at 11 [3.4](a)–(b)(i):

> [A]ny means used for obtaining … information must be proportionate to the gravity of the threat posed and the likelihood of its occurrence … inquiries and investigations into individuals and groups should be undertaken … using as little intrusion into the privacy of affected individuals as is reasonably required …

[147] Ibid 11–12 [3.4](c).

[148] Ibid 13 [4.2].

[149] Ibid 2.

[150] *ASIO Act* (n 116) s 8A(1).

[151] See 'National Security: Finding a Balance', *Q&A* (Australian Broadcasting Corporation, 2014) 0:55:26–1:06:38.

[152] *Telecommunications Interception Act* (n 119) s 180F.

makes the MDRR a more attenuated regime than *Schrems II* contemplates.[153] The absence of appropriate limitations in the regime is compounded by the fact that the ASIO, as an exception to the general rule,[154] can access existing and prospective metadata held by telecommunications providers on an ongoing basis, without any regard for privacy considerations, as long as the Director-General of Security, Deputy Director-General of Security, or an authorised ASIO officer seeking access is satisfied that the disclosure would be 'in connection with' the performance by the ASIO of its functions.[155] The absence of clear and precise rules with these authorisations allows the relevant ASIO officer to easily justify the disclosure of metadata held by telecommunications providers with the broadest interpretation of the ASIO's functions.[156]

The *Telecommunications Interception Act* further permits employees of telecommunications providers to make voluntary disclosures of metadata to the ASIO where they encounter metadata they consider as being 'in connection with' the performance by the ASIO of its functions.[157] The opportunity for voluntary disclosures creates the possibility of 'oversupply' of metadata as employees may disclose more than is necessary.[158] This is because there is no obligation under the *Telecommunications Interception Act* that requires telecommunications providers to provide guidance and training for employees to follow when making voluntary disclosures. The *Telecommunications Interception Act* only requires that employees may disclose metadata they consider as being 'in connection with' the ASIO's functions.[159] Given the ASIO's functions are framed in extremely broad terms, employees of telecommunications providers are likely

153 See ibid.

154 Ibid s 180(4). This section provides that authorisation by enforcement agencies for access to prospective information or documents must not be made unless the disclosure is 'reasonably necessary' for the investigation of an offence punishable by imprisonment for at least three years: at s 180(4)(b).

155 Ibid ss 175(3), 176(4).

156 See Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, *Advisory Report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014* (Report, February 2015) 231–2 [6.138]–[6.139] ('*PJCIS Advisory Report*').

157 *Telecommunications Interception Act* (n 119) s 174(1). See also at s 177, which allows voluntary disclosure to an enforcement agency if the disclosure is reasonably necessary for the enforcement of the criminal law, or a law imposing a pecuniary penalty, or for the protection of the public revenue.

158 Sharon Rodrick, 'Accessing Telecommunications Data for National Security and Law Enforcement Purposes' (2009) 37(3) *Federal Law Review* 375, 399.

159 *Telecommunications Interception Act* (n 119) s 174(1).

to err on the side of caution and disclose more sets of metadata, including that of individuals who are not, or are unlikely to become, of interest to the ASIO.[160]

Secondly, the absence of a compulsory deletion requirement for telecommunications providers and enforcement agencies which have accessed metadata produces uses of metadata that go beyond the legislative scope of the regime. Naturally, the absence of a compulsory deletion requirement removes incentives for agencies to implement limitations and safeguards, such as internal compliance requirements to assess or destroy metadata before a set deletion date or justify why certain sets of metadata should be deemed necessary to retain.[161] The Parliamentary Joint Committee on Intelligence and Security ('PJCIS'), for instance, was provided evidence at the MDRR's 2020 review that claimed that agencies do not delete accessed metadata, draw upon it for future investigations and make secondary disclosures to other agencies for suspected breaches of the law.[162] The Inspector-General of Intelligence and Security ('IGIS'), the main body charged with oversight of NIC agencies, also reported that IGIS staff had identified a small number of instances in which ASIO staff retained either telecommunications data or telecommunications interception data that was not relevant to security.[163] Conversely, the lack of a compulsory deletion period means that telecommunications providers could store metadata for an indefinite time should they consider it necessary to use the metadata for their own commercial purposes.[164]

[160] *ASIO Act* (n 116) s 17(1). One of the ASIO's functions is to 'obtain, correlate and evaluate intelligence relevant to security': at s 17(1)(a). Section 4 provides a broad definition of 'security' as the protection of the Australian government and its people from espionage, sabotage, politically motivated violence, the promotion of communal violence, attacks on Australia's defence system, acts of foreign interference, and serious threats to border security.

[161] See *PJCIS Advisory Report* (n 156) 259 [6.217].

[162] Commonwealth, *Parliamentary Debates*, Parliamentary Joint Committee on Intelligence and Security, 7 February 2020, 26 (Shane Butler, Director Electronic Collection, Law Enforcement Conduct Commission), 29 (Sarah Marshall, Executive Director Operations, Australian Commission for Law Enforcement Integrity) ('*PJCIS Parliamentary Debates*'). See also what Jake Blight, Deputy Inspector-General of the Office of the Inspector-General of Intelligence and Security, explained, at 2:

> There's no obligation for [the] ASIO to destroy data — leaving aside data that's been erroneously collected. For data that is lawfully collected there's nothing in the [Act], the guidelines or the archives rules which requires destruction. So there's no noncompliance if it's kept indefinitely. What there is in the ASIO guidelines is a general statement saying that [the] ASIO may keep a large reference dataset.

[163] Inspector-General of Intelligence and Security, *2017–2018 Annual Report* (Report, 24 September 2018) 2, 23.

[164] *PJCIS Parliamentary Debates* (n 162) 2 (Jake Blight, Deputy Inspector-General, Office of the Inspector-General of Intelligence and Security).

Thirdly, the PJCIS stated that

> [w]hether or not telecommunications data retained under [the MDRR] can be effectively secured is critical to assessing whether [the regime] is … proportionate for national security and law enforcement purposes.[165]

Although the PJCIS's statement was made in 2015 prior to the MDRR taking effect, it must be taken more seriously in light of the proliferation of malicious cyber attacks targeted at critical infrastructure, including telecommunications provider networks.[166] In order to prevent unauthorised access to retained metadata, the *Telecommunications Interception Act* requires that telecommunications providers encrypt information being collected and protect it from unauthorised access.[167] However, the *Telecommunications Interception Act* does not specify which encryption protocols telecommunications providers must implement to safeguard retained metadata.[168] The lack of prescribed encryption protocols could result in lowest-common-denominator security standards. For example, the PJCIS recognised the possibility that internet service providers 'will implement the cheapest solution at the expense of security which would lead to this data being easily hacked by any malicious person or organisation'.[169] Separately, while the Office of the Australian Information Commissioner ('OAIC') is responsible for providing ongoing assessments of how telecommunications providers secure retained metadata under the MDRR,[170] it is widely known that the OAIC is under-resourced,[171] and especially limited in resources and skills when 'faced with investigating highly complex data security incidents'.[172] Without appropriate technical expertise, the effectiveness of the

165 *PJCIS Advisory Report* (n 156) 65 [2.194].

166 Australian Cyber Security Centre, *ACSC Annual Cyber Threat Report: 1 July 2020 to 30 June 2021* (Report, 2021) 8, 20.

167 *Telecommunications Interception Act* (n 119) s 187BA.

168 Ibid.

169 *PJCIS Advisory Report* (n 156) 66 [2.196], quoting Tom Courtney, Submission No 23 to Parliamentary Joint Committee on Intelligence and Security, *Inquiry into Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014* (29 December 2014).

170 Office of the Australian Information Commissioner, Submission No 34 to Parliamentary Joint Committee on Intelligence and Security, *Review of the Mandatory Data Retention Regime* (July 2019) 7 [15].

171 See *For Your Information* (n 19) 1515–16 [45.2]; Office of the Australian Information Commissioner, Submission to Attorney-General's Department, *Review of the Privacy Act 1988 (Cth)* (11 December 2020) 120 [9.6] ('OAIC Privacy Act Submission').

172 Jodie Signato and Mark Burdon, 'The Privacy Commissioner and Own-Motion Investigations into Serious Data Breaches: A Case of Going through the Motions?' (2015) 38(3) *University of New South Wales Law Journal* 1145, 1178.

OAIC's role in enforcing data security standards is further reduced given the increasingly sophisticated nature of malicious actors based overseas.[173]

The MDRR's security protocol is inadequate when having regard to the CJEU's ruling in *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources* ('*Digital Rights Ireland*').[174] The CJEU in *Digital Rights Ireland* invalidated the EU's *Data Retention Directive* ('*DRD*'),[175] which obliged EU member states to provide for the retention of metadata by telecommunication providers for six to 24 months.[176] Although the EU's *DPD* required member states to adopt 'appropriate' technical and organisational standards for data protection,[177] the CJEU held that the *DRD* did not 'ensure effective protection of the [metadata] retained against the risk of abuse and against any unlawful access and use of that [metadata]', as required by art 8 of the *EU Charter*.[178] Regarding the absence of data security measures, the CJEU found that the *DRD* did not set out rules which were specifically adapted to a number of considerations in respect of the retained metadata, including the vast quantity, sensitive nature and risk of unlawful access to the metadata.[179] The CJEU then pointed to the provisions in the *DRD* which allowed telecommunications providers to have regard to economic considerations, including the costs of implementing security measures when determining appropriate data security measures for their networks.[180] While the CJEU's decision is not binding in Australia, the MDRR faces the same weaknesses. Like the EU's *DRD*, the *Telecommunications Interception Act* does not specify which encryption protocols telecommunications providers must implement to ensure data security. It follows that the absence of prescribed security protocols suggests that the MDRR is not proportionate to the regime's legitimate aims.

173 See ibid 1181.

174 *Digital Rights Ireland* (n 1).

175 Ibid [71]; *Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the Retention of Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communications Services or of Public Communications Networks and Amending Directive 2002/58/EC* [2006] OJ L 105/54 ('*DRD*').

176 *DRD* (n 175) arts 5–6.

177 Ibid art 17(1).

178 *Digital Rights Ireland* (n 1) [66].

179 Ibid.

180 Ibid [67].

C *Right to an Effective Remedy under art 47 of the* EU Charter

The second threshold question concerns whether non-citizens are provided effective legal remedies against the misuse of their personal data by the ASD and ASIO under art 47 of the *EU Charter*. Obviously, an individual may only have legal recourse against public authorities if they have sufficient knowledge of the actual circumstances of the misuse of their personal data. The implication here is that not only does an individual need to be aware of being the target of NIC agency activities, the access and use of their personal data must also be unlawful under a law of the Commonwealth or a state or territory. As established in the preceding sections, there will be no 'misuse' of non-citizens' personal data by the ASD and ASIO in circumstances where the access and use of the personal data is necessary for the proper performance of their functions and is authorised by the relevant statutory power. Nevertheless, the following sections demonstrate that there are limited circumstances where non-citizens have legal recourse against the misuse of their personal data in Australia. This second threshold question is split into two inquiries: (i) whether non-citizens can access information regarding the access and use of their personal data in relation to each case study; and (ii) whether there is an independent oversight body with binding authority over the ASD and ASIO and with power to provide rights that are 'substantially equivalent' to those under the *EU Charter*. This section deals with the three case studies together and will draw out differences where relevant.

1 *Access to Sufficient Information*

Due to the inherent secrecy of NIC activities and operations, individuals that are targeted by NIC agencies face insurmountable barriers to accessing any information about the access and use of their personal data.[181] Obviously, covert surveillance means that the target of the surveillance is not and will not be aware of the surveillance. In Lyria Bennett Moses and Louis de Koker's study of the use of data and data analytics amongst NIC agencies, they explain that

> [while] transparency is crucial to sustain democratic controls over government, particularly in the context of data practices, it is also recognised that some

[181] *Intelligence Services Act* (n 112) s 40(1)(a) prohibits the communication of 'any information or matter that was … prepared by or on behalf of the ASD in connection with its functions'. These provisions apply to a person who: is a current or former staff member of the ASD; has entered into a contract, agreement or arrangement with the ASD; or has been an employee or agent of a person who has entered into a contract, agreement or arrangement with the ASD: at s 40(1)(b). Similarly, it is an offence under s 18 of the *ASIO Act* (n 116) for an ASIO employee or agent to convey information acquired in the course of his or her duties outside the ASIO without the authority of the Director-General of Security.

> aspects of government require a level of confidentiality or secrecy to support operational effectiveness.[182]

In light of the need to balance transparency and secrecy in any societal construct, this section examines relevant legislation upholding the idea of transparent government and the *Privacy Act*, including the Australian Privacy Principles ('APPs') and notifiable data breach ('NDB') scheme set out in the *Privacy Act*.

(a) Government Transparency Legislation

The *Freedom of Information Act 1982* (Cth) ('*FOI Act*') provides every individual including non-citizens a legally enforceable right to obtain access to a document of an agency or an official document of a Minister in accordance with the *FOI Act*.[183] However, the ASD and ASIO, as well as any documents that originate with or were received from both of these agencies, are exempt from the operation of the *FOI Act*.[184] Part IV of the *FOI Act* also sets out matters which will give rise to the exemption of certain types of documents from public access. Exempt documents include documents affecting national security, defence or international relations.[185] Individuals, therefore, are unable to access documents regarding NIC agency intelligence activities and operations in order to uncover potential misuses of their personal data as those documents directly relate to the exempt matters.

The ASD and ASIO are subject to the *Public Interest Disclosure Act 2013* (Cth) ('*PID Act*').[186] The *PID Act* encourages and facilitates the reporting of wrongdoing by public officials in the Commonwealth public sector.[187] It is highly unlikely, however, that information about any misuse of non-citizens' personal data would be disclosed to those individuals. This is because a disclosure will only be a public interest disclosure under the *PID Act* if the disclosure is made to an 'authorised internal recipient, or a supervisor of the discloser', and the 'information tends to show, or the discloser believes on reasonable grounds that the information tends to show, one or more instances of disclosable conduct'.[188] Disclosable conduct includes conduct engaged in by an agency or

[182] Lyria Bennett Moses and Louis de Koker, 'Open Secrets: Balancing Operational Secrecy and Transparency in the Collection and Use of Data by National Security and Law Enforcement Agencies' (2017) 41(2) *Melbourne University Law Review* 530, 538.

[183] *Freedom of Information Act 1982* (Cth) s 11.

[184] Ibid sch 2 pt 1 div 1.

[185] Ibid s 33.

[186] *Public Interest Disclosure Act 2013* (Cth) s 72 ('*PID Act*').

[187] Ibid s 6(b).

[188] Ibid s 26(1) item 1.

public official that 'contravenes a law of the Commonwealth'.[189] There would not be any 'disclosable conduct' that would amount to a public interest disclosure because the ASD and ASIO's access and use of personal data is lawful as long as such access and use are necessary for the proper performance of their functions and are authorised by the relevant statutory power.[190]

The Ombudsman under the *Ombudsman Act 1976* (Cth) ('*Ombudsman Act*') has the power to inspect the records mandatorily kept by law enforcement agencies.[191] For example, the Ombudsman may assess whether law enforcement agencies are compliant and have used their statutory powers in line with the objectives of the MDRR.[192] The ASIO, however, is excluded from the operation of the *Ombudsman Act*.[193] Nor is the ASIO required to report to Ministers on individual data access authorisations under the *Telecommunications Interception Act*. The ASD is covered by the *Ombudsman Act*, although in practice, individuals seeking to make complaints about the ASD are referred to the IGIS.[194] Still, the Ombudsman is not authorised to investigate any action taken by a Minister.[195] It follows that the grounds on which signals collection on Australian citizens is authorised by the Minister for Defence under the *Intelligence Services Act* are not reviewable and excluded from the Ombudsman's purview.[196] Given there are no limitations on the ASD's collection of signals intelligence on non-citizens, these activities would also not be reviewable by the Ombudsman. Even if the ASD held information about misuses of non-citizens' personal data, the Attorney-General can prevent the Ombudsman from accessing information if he or she certifies that disclosure of that information would be contrary to the public interest because it would 'prejudice the security, defence or international relations of the Commonwealth'.[197]

189 Ibid s 29(1) item 1. Section 2B of the *Acts Interpretation Act 1901* (Cth) states that, in any Act, the term 'contravene' includes 'fail to comply with'.

190 *PID Act* (n 186) s 33.

191 *Ombudsman Act 1976* (Cth) s 9 ('*Ombudsman Act*'). See also *Telecommunications Interception Act* (n 119) ss 176A(1)(a), 186B.

192 Commonwealth Ombudsman, *A Report on the Commonwealth Ombudsman's Inspection of the Australian Federal Police under the Telecommunications (Interception and Access) Act 1979* (Report, October 2017) 4 [1.7].

193 *Telecommunications Interception Act* (n 119) ss 176A(1), 186B.

194 *For Your Information* (n 19) 1180 [34.56].

195 *Ombudsman Act* (n 191) s 5(2)(a).

196 Ibid.

197 Ibid s 9(3)(a).

(b) Australian Privacy Principles

Although the *Privacy Act* protects non-citizens whose personal data is transferred to and processed in Australia, the ASD and ASIO are completely exempt from the operation of the *Privacy Act*, including the APPs.[198] The APPs are contained in sch 1 of the *Privacy Act* and set out standards that deal with the collection, use, disclosure and storage of personal information. The IGIS has stated that one of the reasons for the exemption of intelligence agencies is that 'it is necessary for the agencies to protect their sources, capabilities and methods if they are to function effectively'.[199] Section 7(1)(f) of the *Privacy Act* provides that an act or practice 'in relation to a record that has originated with, or has been received from an intelligence agency [including the ASD and ASIO]' is not subject to the *Privacy Act*. In addition, s 7(1A) states that the disclosure of personal information by another entity to the ASD and ASIO is not an act or practice which is captured by the *Privacy Act*.[200] The effect of s 7(1A) is that information exchanges between telecommunications providers and the ASIO under the MDRR are exempt from the protections in the *Privacy Act*. The ASD and ASIO are also exempt from certain transparency-promoting APPs and are not obliged to report NDBs to the OAIC or affected individuals under the NDB scheme.[201] Nevertheless, the APPs and NDB scheme under the *Privacy Act* are described as they relate to telecommunications providers.[202]

Non-citizens may access limited information regarding unauthorised access and use of their metadata held by telecommunications providers under the MDRR. Metadata retained under the *Telecommunications Interception Act* is considered 'personal information' for the purposes of the *Privacy Act*.[203] The APPs contain transparency-promoting privacy principles.[204] For example, APP 1.2(a) requires that telecommunications providers take reasonable steps in the circumstances to implement 'practices, procedures and systems relating to the entity's functions or activities' to ensure the privacy of personal information they collect, use and store.[205] In this regard, APP 1.2(b) stipulates that such 'practices, procedures and systems' must be sufficient to 'enable the entity

198 *Privacy Act 1988* (Cth) ss 7(1)(a)(i)(B), (1A) ('*Privacy Act*').

199 Ian Carnell, 'Trust and the Rule of Law' (2005) 14(2) *Journal of the Australian Institute of Professional Intelligence Officers* 5, 7.

200 *Privacy Act* (n 198) s 7(1A).

201 Ibid s 7(1)(a)(i)(B).

202 Ibid pt IIIC, sch 1.

203 *Telecommunications Interception Act* (n 119) s 187LA(2).

204 *Privacy Act* (n 198) sch 1 cls 1, 5, 10, 12–13.

205 Ibid sch 1 cl 1.2(a).

to deal with inquiries or complaints from individuals about the entity's compliance with the [APPs]'.[206] APP 1 may support a non-citizen's inquiry to a telecommunications provider as to whether their metadata has been improperly accessed or mishandled under the MDRR. To that end, individuals may only receive information in those circumstances and not whether their metadata has been misused by the ASIO and enforcement agencies in the course of their investigations.

(c) Notifiable Data Breach Scheme

The NDB scheme is limited to notifying individuals about internal and external data breaches involving their personal information.[207] The notification requirement binding upon telecommunications providers applies where there is an eligible data breach. An eligible data breach may occur where 'there is unauthorised access to, or unauthorised disclosure of, the information' and 'a reasonable person would conclude that the access or disclosure would be likely to result in serious harm to any of the individuals to whom the information relates', or where the information is lost in circumstances where 'unauthorised access to, or unauthorised disclosure of, the information is likely to occur' and

> a reasonable person would conclude that the access or disclosure would be likely to result in serious harm to any of the individuals to whom the information relates …[208]

Telecommunications providers are required to notify the OAIC and individuals whose metadata is involved in the breach and to recommend remedies.[209] Non-citizens, thus, will only be notified in limited circumstances such as where their personal data is lost by telecommunications providers, mistakenly provided to another individual, or subjected to unauthorised access by a malicious third party. Similar to the position of non-citizens under the APPs, non-citizens will not be notified if their metadata has been misused by the ASIO and law enforcement agencies in the course of their investigations.[210]

206 Ibid sch 1 cl 1.2(b).

207 Ibid s 26WE(2), as inserted by *Privacy Amendment (Notifiable Data Breaches) Act 2017* (Cth) sch 1 cl 3; *Telecommunications Interception Act* (n 119) s 187LA. The rationale for data breach notification requirements has been described as recognising 'that "individuals need to know when their personal information has been put at risk in order to mitigate potential identity fraud damages"': *For Your Information* (n 19) 1669 [51.7], quoting Canadian Internet Policy and Public Interest Clinic, *Approaches to Security Breach Notification* (White Paper, 9 January 2007) 2.

208 *Privacy Act* (n 198) ss 26WE(2)(a)(ii), (b)(ii).

209 Ibid ss 26WK–26WL.

210 Ibid s 26WN.

2 *Access to an Independent Oversight Body with Binding Authority*

The second inquiry of the second threshold question concerns whether there is an independent oversight body with binding authority over NIC agencies and with the power to provide non-citizens rights that are '*substantially equivalent*' to those under the *EU Charter*. The oversight body must also be able to provide individuals remedies such as access to their personal data or the rectification or erasure of the personal data.[211]

Even if non-citizens have sufficient knowledge about any misuse of their personal data by NIC agencies, there is no redress mechanism under the *Intelligence Services Act* which would allow individuals to challenge the ASD's signals intelligence collection. Similarly, there is no redress mechanism under the *Telecommunications Interception Act* in relation to the MDRR. The ASIO's issuance of foreign intelligence collection warrants and individual data access authorisations in accordance with the *Telecommunications Interception Act* is exempt from the *Administrative Decisions (Judicial Review) Act 1977* (Cth).[212] Even if judicial review of these decisions were pursued under s 75(v) of the *Constitution* or s 39B of the *Judiciary Act 1903* (Cth), the ASIO's access of the relevant communications would have already taken place before discovery by any individual.

There are limited avenues for non-citizens to make complaints in respect of the ASD's signals intelligence collection and the ASIO's collection of foreign intelligence. Ordinarily, the IGIS provides oversight over the legality and propriety of the operations of intelligence agencies, including the ASD and ASIO.[213] However, the operation of the IGIS is subject to some limitations. The IGIS's oversight powers are not extraterritorial and its ability to respond to a complaint is limited to the extent that Australian citizens or permanent residents are affected, or an Australian law may be violated.[214] Similarly, the PJCIS, which is appointed under the *Intelligence Services Act* to ensure, among other things, 'national security legislation remains necessary, proportionate and effective by conducting statutory reviews'[215] is excluded from 'reviewing an aspect of the activities of [the] ASIO [or] ASD … that [do] not affect an Australian

211 *Schrems II* (n 1) [194], [197].

212 *Administrative Decisions (Judicial Review) Act 1977* (Cth) sch 1 para (d).

213 *Inspector-General of Intelligence and Security Act 1986* (Cth) s 8 ('*IGIS Act*').

214 Ibid s 8(4).

215 'Role of the Committee', *Parliament of Australia* (Web Page) <https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/Role_of_the_Committee>, archived at <https://perma.cc/QQ8T-SB9N>. See also *Intelligence Services Act* (n 112) ss 28–9.

person'.[216] Further, the Office of the Independent National Security Legislation Monitor ('INSLM'), on his or her own initiative, provides independent review and reporting on the operation, effectiveness and implications of the statutory powers of the ASD and ASIO, including by reference to whether the statutory powers contain 'appropriate safeguards for protecting the rights of individuals'.[217] However, the INSLM is yet to report on the statutory powers of the ASD and ASIO in the context of their implications on the privacy interests of non-citizens.[218]

It must also be noted that the IGIS would arguably not be considered independent under art 8(3) of the *EU Charter* on the basis that the IGIS is accountable to Ministers.[219] The guarantee of independence of the oversight body within the meaning of art 8(3) is intended to ensure effective and reliable monitoring of compliance with the rules on the protection of individuals' privacy interests.[220] With regard to the ministerial accountability framework of intelligence agencies, Keiran Hardy and George Williams argue that expanding the powers of intelligence agencies is perceived as granting a clear political benefit to politicians,[221] such that, as the Human Rights Law Centre has submitted:

> [It] is not in the interests of the Attorney-General or other Ministers in Government to reveal important details of misconduct and illegality of intelligence agencies …[222]

The IGIS's annual report, for example, must be provided to the Leader of the Opposition as well as the Attorney-General, and an edited form of the report must be tabled before both Houses of Parliament and made public via the

[216] *Intelligence Services Act* (n 112) s 29(3)(e). Regardless, the PJCIS is not empowered to review the ASD and ASIO's operational matters, limiting its ability to review and assess reports from the IGIS: at ss 29(3)(a)–(b).

[217] *Independent National Security Legislation Monitor Act 2010* (Cth) s 6(1)(b)(i). See also at s 6(1)(a)(i).

[218] 'Reviews and Reports', *Independent National Security Legislation Monitor* (Web Page) <https://www.inslm.gov.au/reviews-reports>, archived at <https://perma.cc/9SJF-RZBF>.

[219] See *IGIS Act* (n 213) ss 8, 9–9AA.

[220] See *Digital Rights Ireland* (n 1) [68]; *GDPR* (n 4) recital 11.

[221] Keiran Hardy and George Williams, 'Executive Oversight of Intelligence Agencies in Australia' in Zachary K Goldman and Samuel J Rascoff (eds), *Global Intelligence Oversight: Governing Security in the Twenty-First Century* (Oxford University Press, 2016) 315, 334.

[222] Human Rights Law Centre, Submission to Attorney-General's Department, *Comprehensive Review of the Legal Framework of the National Intelligence Community* (12 December 2018) 7.

Commonwealth's Transparency Portal.[223] The disclosure of information that is withheld from Parliament and the public ultimately rests within the sole discretion of the responsible Minister or, in the case of the annual report, the Attorney-General.[224] Consequently, there is little 'way of knowing what the basis for omitting such details, or entire IGIS reports from public view, is'.[225]

D *Conclusion*

To summarise briefly, the statutory powers granted to the ASD and ASIO in these case studies are not limited to what is 'strictly necessary' in terms of art 52(1) and do not ensure effective judicial protection for EU citizens under art 47 of the *EU Charter*. As a result, the statutory powers examined would likely be held to interfere with the rights to privacy and data protection under arts 7 and 8 of the *EU Charter*. Of particular significance is that the statutory powers in relation to the ASD's signals intelligence collection and the ASIO's collection of foreign intelligence about non-citizens in Australia demarcate and apportion protections according to individuals' citizenship. The critical implication, thus, is that non-citizens are afforded significantly fewer protections in comparison to Australian citizens or permanent residents subject to similar activities by the ASD and ASIO.

IV Australia's Adequacy Prospects under the *GDPR*

Part IV argues that any reforms proposed as part of moving towards adequacy under the *GDPR* must consider the breadth of NIC agencies' electronic surveillance powers as judged in light of the *Schrems II* ruling. This Part also posits that the case studies reflect the consequentialist treatment of privacy protection in Australia, particularly with regard to successive federal governments' reluctance towards adopting a general right to privacy.

[223] *IGIS Act* (n 213) s 35; *Public Governance, Performance and Accountability Act 2013* (Cth) s 46; *Public Governance, Performance and Accountability Rule 2014* (Cth) s 17ABA; 'Digital Annual Reporting Tool: Frequently Asked Questions', *Department of Finance* (Web Page, 20 September 2021) <https://www.finance.gov.au/digital-annual-reporting-tool-frequently-asked-questions>, archived at <https://perma.cc/NC8P-7UYN>.

[224] *IGIS Act* (n 213) s 35(5). The Attorney-General

> may make such deletions from a report … as the Attorney-General considers necessary in order to avoid prejudice to security, the defence of Australia, Australia's relations with other countries, law enforcement operations or the privacy of individuals.

[225] Human Rights Law Centre (n 222) 7.

A *Electronic Surveillance Laws as Likely Barriers to an Adequacy Decision*

The CJEU's ruling in *Schrems II* casts doubt on the possibility of Australia reaching adequacy under the *GDPR* if it were to seek an adequacy assessment. As the case studies demonstrate, the ASD and ASIO's statutory powers fall considerably short of providing 'essentially equivalent' protections to those guaranteed under EU law. Of greater concern is that the case studies only provide a small sample of the vast breadth of electronic surveillance laws in Australia. Other statutory powers that authorise NIC agencies to access and use personal data to undertake their functions risk the same criticisms in respect of the absence of limitations and safeguards.[226] Indeed, the *Richardson Review* found that Australia had, in general, more extensive and intrusive powers with lighter oversight than many other Western liberal democracies.[227] So, it is doubtful that the consumer-law-focused reforms contemplated in the ACCC's Digital Platforms Inquiry or any reforms made with the intention of bringing the *Privacy Act* in alignment with the *GDPR* would be sufficient to meaningfully increase Australia's adequacy prospects. This is because, as discussed in the Part III, NIC agencies and their activities are entirely exempt from the operation of the *Privacy Act*.

Obviously, the EC will not assess the adequacy of third countries solely on the basis of their electronic surveillance laws.[228] However, it is important to recognise that as a consequence of the CJEU's rulings in *Schrems I* and *Schrems II*, the EC has increasingly acknowledged in adequacy decisions the importance of third countries ensuring limitations and safeguards, including oversight and individual redress mechanisms, with regard to access and use of EU citizens' personal data by public authorities. On 28 June 2021, the EC published adequacy decisions for the United Kingdom ('UK') under the *GDPR*[229] and *UK*

[226] See Independent National Security Legislation Monitor, *Trust but Verify: A Report Concerning the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 and Related Matters* (Report No 9, 30 June 2020) 188–99 [10.1]–[10.32].

[227] *Richardson Review* (n 106) vol 1, 42 [3.54].

[228] Cf European Parliament, *European Parliament Resolution of 25 March 2021 on the Commission Evaluation Report on the Implementation of the General Data Protection Regulation Two Years after Its Application (2020/2717(RSP))*, Doc No P9_TA(2021)0111, 25 March 2021. The European Parliament stated that it

> [reiterates] the fact that mass surveillance programmes encompassing bulk data collection prevent adequacy findings; urges the [European] Commission to apply the conclusions of the CJEU in the cases *Schrems I*, *II* and *Privacy International & al* (2020) to all reviews of adequacy decisions as well as ongoing and future negotiations …

at [33] (citations omitted).

[229] *UK Adequacy Decision* (n 29).

Law Enforcement Directive Adequacy Decision.[230] Nearly two thirds of the EC's 68-page adequacy decision for the UK under the *GDPR* is spent on a detailed analysis on the statutory powers granted to UK public authorities to access personal data on law enforcement and national security grounds.[231] Similarly, the EC's adequacy decisions for South Korea and Japan, adopted on 17 December 2021 and 23 January 2019, respectively, also contain a comprehensive assessment on governmental access to personal data.[232] By comparison, the EC's adequacy decisions for Argentina, Israel, New Zealand and Uruguay, which were all published prior to the *Schrems* decisions, do not contain the same extent of

[230] *UK Law Enforcement Directive Adequacy Decision* (n 29); *Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data by Competent Authorities for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and on the Free Movement of Such Data, and Repealing Council Framework Decision 2008/977/JHA* [2016] OJ L 119/89.

[231] *UK Adequacy Decision* (n 29) recitals 112–272. The EC's extensive assessment is perhaps due to the EDPB's earlier opinion of the UK draft adequacy decision under the *GDPR* (n 4) which called on the EC to examine and monitor the UK's surveillance powers, including the bulk interception of communications and overseas disclosure of data on national security exemptions: European Data Protection Board, *Opinion 14/2021 regarding the European Commission Draft Implementing Decision Pursuant to Regulation (EU) 2016/679 on the Adequate Protection of Personal Data in the United Kingdom*, 13 April 2021, 34 [145], 40 [173]–[174], 45 [190]. The EDPB's role in the context of the EC's adequacy decision assessments is significant. Article 70(1)(s) of the *GDPR* (n 4) states that one of the EDPB's functions is to

> provide the Commission with an opinion for the assessment of the adequacy of the level of protection in a third country or international organisation, including for the assessment whether a third country, a territory or one or more specified sectors within that third country, or an international organisation no longer ensures an adequate level of protection. To that end, the Commission shall provide the Board with all necessary documentation, including correspondence with the government of the third country, with regard to that third country, territory or specified sector, or with the international organisation.

See also Article 29 Working Party, 'Adequacy Referential' (Working Document No WP 254 rev.01, 6 February 2018) ch 2:

> [T]he information provided by the [EC] should be exhaustive and put the EDPB in a position to make an own assessment regarding the level of data protection in the third country. The EDPB will provide an opinion on the [EC's] findings in due time and … identify insufficiencies in the adequacy framework, if any. The EDPB will also endeavour to propose alterations or amendments to address possible insufficiencies.

[232] *Commission Implementing Decision of 17.12.2021 Pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the Adequate Protection of Personal Data by the Republic of Korea under the Personal Information Protection Act*, Doc No C(2021) 9316, 17 December 2021, recitals 139–208; *Commission Implementing Decision (EU) 2019/419 of 23 January 2019 Pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the Adequate Protection of Personal Data by Japan under the Act on the Protection of Personal Information* [2019] OJ L 76/1, recitals 113–75.

consideration relative to the length of their respective decisions.[233] Accordingly, the EC, at a minimum, will continue to consider the electronic surveillance laws of third countries in adequacy decisions, in addition to the factors contemplated under recital 104 and art 45(2)(a) of the *GDPR*.

B *The Absence of a General Right to Privacy*

As recounted earlier, consequentialist accounts of privacy are variable, such that the value of protecting individual privacy interests hinges on what is considered desirable for society in the circumstances. The inadequate standard of privacy protection in light of the *Schrems II* ruling reflects the consequentialist treatment of privacy protection in Australia. As explained in the *Richardson Review*, access to and use of personal data by NIC agencies are justified in Australia's national interest:

> In Australia's case, it collects intelligence for the protection, prosperity and advancement of a liberal democracy. Intelligence activities that serve these purposes are governed by a utilitarian ethic: they advance the greater good of the national interest of a liberal democratic society. But the national interest can be a blunt instrument and it does not always accommodate values such as individual rights or finer ethical considerations.[234]

Individual privacy interests, thus, are trumped by the overarching goal of collective security on the basis that security produces desirable outcomes for society. When Australia's approach to privacy protection is understood in consequentialist terms, it becomes clear that other aspects of Australia's privacy law regime may attract scrutiny in an adequacy assessment. Having regard to the EU's deontological commitment in respect of privacy and data protection as fundamental rights, one weakness with Australia's privacy law regime may be the lack of constitutional or statutory privacy rights.

[233] *Commission Decision of 30 June 2003 Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequate Protection of Personal Data in Argentina* [2003] OJ L 168/19; *Commission Decision of 31 January 2011 Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequate Protection of Personal Data by the State of Israel with Regard to Automated Processing of Personal Data* [2011] OJ L 27/39; *Commission Implementing Decision of 19 December 2012 Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequate Protection of Personal Data by New Zealand* [2013] OJ L 28/12; *Commission Implementing Decision of 21 August 2012 Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequate Protection of Personal Data by the Eastern Republic of Uruguay with Regard to Automated Processing of Personal Data* [2012] OJ L 227/11.

[234] *Richardson Review* (n 106) vol 1, 164 [7.46].

Of course, pursuing collective security over recognising individual privacy rights is not unique to Australia or its 'Five Eyes' intelligence sharing alliance partners — Canada, New Zealand, the UK and the US.[235] National security is an important and legitimate aim used to protect states and should be given pre-eminence, subject to appropriate limitations and safeguards. However, successive federal governments' reticence towards adopting a general right to privacy makes Australia an outlier amongst its Five Eyes partners.[236] The absence of a general right to privacy limits individuals' ability to challenge the lawfulness of potentially excessive electronic surveillance laws and therefore undermines the appropriate balance to be struck between, on the one hand, the efficiency and effectiveness of surveillance measures and, on the other hand, the need to protect individuals' privacy interests.

Indeed, the EC may likely consider a third country's respect for human rights and fundamental freedoms, as well as international commitments entered into, in an adequacy assessment.[237] In the UK's adequacy decision, for example, the EC noted that the *Human Rights Act 1998* (UK) incorporated the rights contained in the *ECHR* into the law of the UK, including 'the right to respect for private and family life (and the right to data protection as part of that right)'.[238] In this regard, Australia's ratification of the *International Covenant on Civil and Political Rights* ('*ICCPR*')[239] in 1980 is relevant.[240] Article 17 of the *ICCPR* provides that '[n]o one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation'.[241] The *ICCPR*, including the *Universal*

[235] The *British–US Communication Intelligence Agreement*, United Kingdom–United States (5 March 1946) (also known as the *UKUSA Agreement*) is a treaty for cooperation in signals intelligence between the UK and US, with Australia, Canada and New Zealand later joining (collectively, the so-called 'Five Eyes'): 'A Brief History of the UKUSA Agreement', *GCHQ* (Web Page, 5 March 2021) <https://www.gchq.gov.uk/information/brief-history-of-ukusa>, archived at <https://perma.cc/736S-KD4W>.

[236] See Brendan Walker-Munro, 'A Shot in the Dark: Australia's Proposed Encryption Laws and the "Disruption Calculus"' (2019) 40(3) *Adelaide Law Review* 783, 794; Alana James, 'Government Mass Surveillance and Law in the Five Eyes Countries' (PhD Thesis, University of Melbourne, 2018) 5.

[237] *GDPR* (n 4) art 45(2)(a).

[238] *UK Adequacy Decision* (n 29) recital 10.

[239] *International Covenant on Civil and Political Rights*, opened for signature 16 December 1966, 999 UNTS 171 (entered into force 23 March 1976) ('*ICCPR*').

[240] 'International Covenant on Civil and Political Rights', *United Nations* (Web Page, 12 March 2022) <https://treaties.un.org/pages/ViewDetails.aspx?src=IND&mtdsg_no=IV-4&chapter=4&clang=_en>, archived at <https://perma.cc/WV35-X9XW>.

[241] *ICCPR* (n 239) art 17(1).

Declaration of Human Rights ('*UDHR*'),[242] which provides a similar provision in art 12, directly or indirectly prompted judicial recognition of a right to privacy in Canada, New Zealand, and the UK.[243] However, successive federal governments have refrained from introducing a national, judicially enforceable bill of rights that would implement art 17 of the *ICCPR* (and, by extension, art 12 of the *UDHR*).[244] The absence of a constitutional bill of rights, for example, means that the High Court has limited powers to invalidate potentially excessive electronic surveillance laws.[245] As a result, Parliament is left with the exclusive role of assessing laws against human rights standards, leaving little room for judicial involvement.

In 1988, the Office of the United Nations High Commissioner for Human Rights announced the right to privacy in art 17 of the *ICCPR* was to apply to states, natural persons, and legal persons, and that all member states were required to give effect to the protection of the right.[246] In response, the federal government enacted the *Privacy Act* to give effect to art 17 of the *ICCPR* and Australia's agreement to implement the Organisation for Economic Co-Operation and Development Guidelines on the Protection of Privacy and Transborder Flows of Personal Data ('OECD Guidelines').[247] Privacy scholars, however, have pointed out that the enactment of the *Privacy Act* followed Australia's agreement to implement the OECD Guidelines, which were based on strengthening the free flow of personal information across member countries and were

[242] *Universal Declaration of Human Rights*, GA Res 217A (III), UN GAOR, UN Doc A/810 (10 December 1948).

[243] See *Human Rights Act 1998* (UK) sch 1 art 8(1); *New Zealand Bill of Rights Act 1990* (NZ) s 21; *Canada Act 1982* (UK) sch B pt I s 8.

[244] See Australian NGO Coalition, 'Australia's Compliance with the International Covenant on Civil and Political Rights', Submission to the Human Rights Committee, September 2017, 9–10; David Lindsay, 'Protection of Privacy under the General Law Following ABC v Lenah Game Meats Pty Ltd: Where to Now?' (2002) 9(6) *Privacy Law and Policy Reporter* 101, 107. David Lindsay articulated the principal arguments for a bill of rights in respect of according privacy the status of a human right. Although acknowledging that a bill of rights is not a panacea, he argued:

> First, it would ensure that fundamental rights or interests, such as privacy, are at the forefront of judicial decision-making, rather than in the background. Second, it would provide a framework for the development of principles for balancing rights and interests that may come into conflict. Third, and relatedly, it would provide a framework for the principled and consistent development of substantive areas of the general law, including the application of the substantive law to the media.

[245] Hardy and Williams (n 221) 316.

[246] Human Rights Committee, 'General Comment Number 16: Article 17 (Right to Privacy)' in *Compilation of General Comments and General Recommendations Adopted by Human Rights Treaty Bodies*, UN Doc HRI/GEN/1/Rev.9 (27 May 2008) vol 1, 191.

[247] *Privacy Act* (n 198) Preamble, s 2A(h); OAIC Privacy Act Submission (n 171) 21 [1.3].

not an express attempt to address the human rights considerations contemplated in the *ICCPR*.[248] That view remains embodied in the statutory scheme of the *Privacy Act* to date.[249] The *Privacy Act* performs a rather instrumental function in governing the proper use and access of personal information and 'does not prescribe privacy rights to individuals per se'.[250] Further, given the *ICCPR* has not been given effect by separate domestic legislation, Australian citizens lack a direct cause of action under the right to privacy provided for in the *ICCPR*.[251]

In short, the absence of a general right to privacy could be singled out by the EC, especially as the privacy law regimes of three of Australia's Five Eyes partners — Canada, New Zealand and the UK — are considered *adequate* under the *GDPR* and have their respective forms of a right to privacy.

V Conclusion

This article covers a timely and important issue — the extent to which the CJEU's ruling in *Schrems II* could impact Australia's adequacy decision prospects. The issue of adequacy under the *GDPR* is attracting attention in the recent *Privacy Act* reform discourse, namely, in the ACCC's final report for the Digital Platforms Inquiry and the AGD's review of the *Privacy Act*. However, the present discourse concerning the necessary reforms required for an adequacy decision for Australia is limited to the *Privacy Act*. This article argues that since the CJEU's rulings in *Schrems I* and *Schrems II*, third countries seeking an adequacy decision must ensure limitations and safeguards that are 'essentially equivalent' to those guaranteed under EU law, as regards to the access and use of EU citizens' personal data by public authorities. If the federal government decides to move towards the path of obtaining adequacy under the *GDPR*, the

[248] Roger Clarke, 'The Australian Privacy Act 1988 as an Implementation of the OECD Data Protection Guidelines', *Roger Clarke's Web-Site* (Web Page, 25 June 1989) <http://www.rogerclarke.com/DV/PActOECD.html>, archived at <https://perma.cc/DP6A-98GK>. Roger Clarke points out that the OECD's review of the information privacy laws of its members was based on strengthening the free flow of personal information across countries and was not expressly 'an attempt to flesh out more general documents concerning human rights, such as *ICCPR*': at [3.1].

[249] Lindsay, 'Conceptual Basis of Privacy' (n 31) 165. Lindsay explains that information privacy laws are based on 'purely consequentialist considerations' and tend to become 'focused on improving technocratic procedures of information management, rather than addressing the privacy implications of data processing'.

[250] Mark Burdon and Paul Telford, 'The Conceptual Basis of Personal Information in Australian Privacy Law' (2010) 17(1) *eLaw Journal: Murdoch University Electronic Journal of Law* 1, 12.

[251] Joint Standing Committee on Foreign Affairs, Defence and Trade, Parliament of Australia, *Legal Foundations of Religious Freedom in Australia* (Interim Report, November 2017) 6 [2.6].

position of Australia's NIC agencies and the breadth of their electronic surveillance powers would likely be considered by the EC.

The case studies examined show that the electronic surveillance powers of the ASD and ASIO fail to provide 'essentially equivalent' protections to those guaranteed under EU law. The statutory powers demarcate and apportion protections according to an individual's citizenship. Non-citizens are afforded limited protections and, in some instances, no protections by comparison to Australian citizens or permanent residents subject to similar surveillance activities. In relation to the ASD's collection of foreign signals intelligence on non-citizens overseas, there are no provisions delimiting the scope of the ASD's collection so that interferences with individuals' privacy interests are necessary and proportionate. The significant implication here is that the *bulk* collection and processing of non-citizens' personal data overseas are authorised. That finding is wholly incompatible with the standard of protection required in order to be considered adequate under the *GDPR*.

Again, the electronic surveillance laws of third countries are not the only factors that the EC will consider in an adequacy assessment under the *GDPR*. Given this article is one of the first critical assessments of the implications of the *Schrems II* decision on Australia's adequacy prospects, the author has focused on the position of certain NIC agencies. To that end, the author invites alternative findings or propositions to those made in this article and further scrutiny of the *Schrems II* decision for Australia.